IT-PLANUNGSRAT

19.10.2026

Föderale Zielarchitektur für Postfach- und Kommunikationslösungen

Rechtsgutachten

Eichler Kern Klein Rechtsanwälte PartG mbB & PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH

Das Klammerdokument gibt einen Überblick über die Zielarchitektur und beschreibt abgeleitete strategische Handlungsempfehlungen. Die in der folgenden Tabelle aufgelisteten Begleitdokumente geben einen tieferen Einblick in die im Klammerdokument zusammenfassend dargestellten Inhalte.

Titel	Dokumentenart	Inhalt
Überblick und Handlungsempfehlungen	Klammerdokument	Übergreifende Zusammenfassung des Vorhabens und Darstellung strategischer Implikationen
Zielarchitektur (Version 1.1)	Begleitdokument	Fortschreibung der auf die Ziele des Vorhabens ausgerichteten Zielarchitektur
Übergreifende Transitionsstrategie	Begleitdokument	Transitionsstrategie zur schrittweisen Überführung bestehender Postfachlösungen in die ZaPuK-Infrastruktur
Rechtsgutachten	**Begleitdokument**	**Prüfung der rechtlichen Rahmenbedingungen sowie Ableitung von Handlungsempfehlungen für die Umsetzung**

Herausgeberin und Lizenzgeberin:
FITKO (Föderale IT-Kooperation) Anstalt des öffentlichen Rechts
Erstellt durch:
Dr. Hannah Rubin, Svenja Gutsche, Eichler Kern Klein Rechtsanwälte PartG mbB
Dr. Bernhard Freund, M.Comp.Sc., LL.M. (Wellington), PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH
Nutzungsbedingungen
Dieses Gutachten wird durch die Herausgeberin unter der Creative-Commons-Lizenz **Namensnennung 4.0 International (CC BY 4.0)** zur Verfügung gestellt. Die Lizenz erlaubt insbesondere Vervielfältigung, Verbreitung, öffentliche Zugänglichmachung sowie Bearbeitung, auch zu kommerziellen Zwecken, sofern eine angemessene Namensnennung erfolgt und auf die Lizenz verwiesen wird.
Lizenztext: https://creativecommons.org/licenses/by/4.0/legalcode.de

Inhaltsverzeichnis

A. Sachverhalt 14
I. ZaPuK - Hintergrund und Kontext des Vorhabens 14
II. ZaPuK – Wesentliche Bestandteile und Eckpunkte der Zielarchitektur 15
B. Prüfauftrag 17
C. Lesehilfen: Folgerungen für ZaPuK und Empfehlungen für Rechtsänderungen 19
D. Rechtliche Würdigung 28
I. Verfassungsrechtliche Machbarkeit einer föderal einheitlichen Postfach- und Kommunikationsstruktur 28
1. Verfassungsrechtliche Ausgangslage 28
1.1. Ausgangspunkt I: Kompetenzverteilung in der deutschen Gesetzgebung 28
1.2. Ausgangspunkt II: Kompetenzverteilung in der deutschen Verwaltung 30
1.2.1. Grundsatz: Zuständigkeit der Länder für den Verwaltungsvollzug 30
1.2.2. Bundeseigene Verwaltung 34
1.2.3. Selbstverwaltung der Kommunen 35
1.2.4. Zusammenfassung: Vollzugszuständigkeiten und diesbezügliche Regelungsbefugnisse als Ausgangslage 39
1.3. Ausgangspunkt III: Bei der Regelung und Ausübung der Verwaltungskompetenzen zu beachtende Grundsätze 40
1.3.1. Konnexitätsgrundsatz – Zusammenspiel zwischen Aufgabenordnung und Finanzierung 40
1.3.2. Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung 43
1.3.3. Verbot der Mischverwaltung 44
1.4. Sondervorschrift für die Zusammenarbeit im IT-Bereich: Art. 91c GG 44
1.5. Sondervorschrift für den Bereich der Finanzverwaltung: Art. 108 GG 46
2. Untersuchung potenzieller verfassungsrechtlicher Rechtsgrundlagen für das Vorhaben 48
2.1. Regelungs- und Organisationskompetenz des Bundes bei der Ausführung von Bundesgesetzen (Art. 84-86 GG) 49

2.1.1. Bundeseigene Verwaltung 49
2.1.2. Ausführung von Bundesrecht durch die Länder als eigene Angelegenheit 49
2.1.3. Bundesauftragsverwaltung durch die Länder 50
2.1.4. Folgerungen für die Machbarkeit von ZaPuK 51
2.2. Zusammenarbeit von Bund und Ländern im IT-Bereich (Art. 91c GG) 52
2.2.1. Bundeskompetenz nach Art. 91c Abs. 4 GG – Errichtung und Betrieb eines Verbindungsnetzes 52
2.2.2. Bundeskompetenz nach Art. 91c Abs. 5 GG – Regelung des informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern 55
2.2.3. Zusammenwirken von Bund und Ländern nach Art. 91c Abs. 1 und 2 GG 76
2.2.4. Zusammenwirken von Bund und Ländern im Bereich der Finanzverwaltung 85
2.3. Folgerungen für ZaPuK: Herleitung der rechtlichen Machbarkeit des Gesamtvorhabens durch Zusammenführung der verschiedenen Gesetzgebungs- und Verwaltungskompetenzen 88
3. Grundgesetzänderung zur Umsetzung von ZaPuK 89
II. Verwaltungsverfahrensrechtliche Rahmenbedingungen für die Umsetzbarkeit – Relevante Vorgaben zur digitalen Kommunikation auf Bundesebene 90
1. Eröffnung des Zugangs für elektronische Kommunikation durch Empfänger 92
1.1. Ausgangspunkt: Freiwilligkeitsgrundsatz und Zugangseröffnung 93
1.2. Fehlendes Adressregister für Privatpersonen in der ZaPuK-Architektur 96
1.3. Neuordnung durch das Gesetz für den Bürokratierückbau zum 1. Juli 2027 97
1.4. Sinnvolle Rechtsänderungen 98
1.5. Folgerungen für die Architektur von ZaPuK 99
2. Erklärungen/Nachrichten von Seiten der Behörde 100

2.1. Begriffliche Grundlagen – Zugang, Bekanntgabe, Zustellung 100
2.1.1. Zugang einer Willenserklärung 101
2.1.2. Bekanntgabe von Verwaltungsakten 102
2.1.3. Zustellung 103
2.2. Digitale Bekanntgabe von Verwaltungsakten 104
2.2.1. Elektronische Übermittlung an den Empfänger – dezentraler Backend-Betrieb bei Organisationspostfächern 106
2.2.2. Abruf über öffentlich zugängliche Netze/Bereitstellung zum (Daten-)Abruf – zentraler Backend-Betrieb 113
2.3. Digitale Zustellung von Dokumenten 137
2.3.1. Zustellung gegen Empfangsbekenntnis an einen unbeschränkten Empfängerkreis 138
2.3.2. Zustellung gegen Empfangsbekenntnis an besonders vertrauenswürdige Empfänger 140
2.3.3. Entfallene Möglichkeit einer Zustellung per De-Mail 140
2.3.4. Folgerungen für die Architektur von ZaPuK 141
3. Umsetzung des Schriftformerfordernisses bei elektronischer Kommunikation ... 141
3.1. Bislang geltende Rechtslage 143
3.1.1. Bei an die Behörde gerichteten elektronischen Erklärungen 143
3.1.2. Bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde 144
3.2. Neuordnung durch das Gesetz für den Bürokratierückbau zum 1. Juli 2027 145
3.3. Folgerungen für die Architektur von ZaPuK 147
III. Datenschutzrechtliche Rahmenbedingungen für die Umsetzbarkeit von ZaPuK 147
1. Anwendbares Datenschutzrecht 148
1.1. Unionsrecht 148
1.1.1. Die DSGVO als vorrangiger und weitgehend vereinheitlichter Rahmen. 148

1.1.2. Bereichsausnahme und JI-Richtlinie 150
1.1.3. Schutz elektronischer Kommunikation (ePrivacy) und Verhältnis zur DSGVO 150
1.1.4. Öffnungsklauseln: kein abschließender Charakter der DSGVO 151
1.1.5. Folgerungen für die Architektur von ZaPuK 152
1.2. Nationales Recht 153
1.2.1. Nationales Recht im Gefüge der DSGVO 153
1.2.2. Allgemeines Datenschutzrecht: BDSG und Landesdatenschutzgesetze 154
1.2.3. Bereichsspezifisches Datenschutz- und Geheimnisrecht 155
1.2.4. Datenschutz im Bereich der Justiz und der Strafverfolgung (JI-Recht) 156
1.2.5. Telekommunikations- und telemedienbezogenes Datenschutzrecht 156
1.2.6. Bereichsspezifische Rechtsgrundlagen mit Bezug zur Postfachinfrastruktur 157
1.2.7. Folgerungen für die Architektur von ZaPuK 157
1.3. Anwendbarkeit 158
1.3.1. Ausgangspunkt: weiter Verarbeitungsbegriff, aber relativer Personenbezug 159
1.3.2. Übertragung auf die Datenarten und Rollen in ZaPuK 161
1.3.3. Folgerungen für die Architektur von ZaPuK 165
2. Datenschutzrechtliche Rollen 167
2.1. Die datenschutzrechtlichen Rollen der DSGVO 168
2.1.1. Der Verantwortliche und die Wege zur Verantwortlichkeit 168
2.1.2. Gemeinsame Verantwortlichkeit 169
2.1.3. Abgrenzung zur Auftragsverarbeitung 170
2.2. Übertragung auf die verteilte Architektur von ZaPuK 170
2.2.1. Ausgangspunkt: Was ist personenbezogen? 171

2.2.2. Rollen der einzelnen Akteure ... 171
2.2.3. Raum-Management-Service und technische Nutzer ... 172
2.2.4. Zentrale Querschnittskomponenten ... 172
2.2.5. Verantwortlichkeit im verteilten Betrieb ... 173
2.2.6. Absicherung der Metadatentrennung ... 174
2.3. Folgerungen für die Architektur von ZaPuK ... 175
3. Grundsätze des Datenschutzes ... 176
3.1. Rechtmäßigkeit ... 176
3.1.1. Der Rechtmäßigkeitsgrundsatz und das Verbot mit Erlaubnisvorbehalt ... 177
3.1.2. Zwei Ebenen der Verarbeitung: fachliche Verarbeitung und Infrastrukturbetrieb ... 178
3.1.3. Rechtsgrundlagen der Beteiligten ... 179
3.1.4. Besondere Kategorien personenbezogener Daten ... 180
3.1.5. Rechtsgrundlage für den Infrastrukturbetrieb: Auffangnorm oder spezialgesetzliche Grundlage ... 181
3.1.6. Erforderlichkeit als übergreifender Maßstab ... 182
3.1.7. Folgerungen für die Architektur von ZaPuK ... 182
3.2. Zweckbindung ... 183
3.2.1. Zweckfestlegung und Weiterverarbeitungsverbot ... 184
3.2.2. Zweckänderung und Weiterverarbeitung ... 185
3.2.3. Bereichsspezifische Verschärfungen und das OZG als Vorbild ... 185
3.2.4. Übertragung auf ZaPuK ... 186
3.2.5. Folgerungen für die Architektur von ZaPuK ... 188
3.3. Datenminimierung ... 189
3.3.1. Inhalt und Abgrenzung des Grundsatzes ... 190
3.3.2. Bereichsspezifische Ausprägungen ... 191
3.3.3. Übertragung auf ZaPuK ... 191
3.3.4. Folgerungen für die Architektur von ZaPuK ... 193

3.4. Richtigkeit ... 195
3.4.1. Inhalt und Abgrenzung des Grundsatzes ... 195
3.4.2. Übertragung auf ZaPuK ... 196
3.4.3. Folgerungen für die Architektur von ZaPuK ... 197
3.5. Speicherbegrenzung ... 199
3.5.1. Löschung und Archivierung ... 199
3.5.2. Logdaten ... 205
3.6. Integrität und Vertraulichkeit (Datensicherheit) ... 211
3.6.1. Integrität: systemseitig sicherstellen oder kryptografisch? ... 212
3.6.2. Vertraulichkeit der Inhalte durch Verschlüsselung ... 217
3.6.3. Vertraulichkeit der Kommunikationsbeziehung (Metadatenschutz) 253
4. Rechenschaftspflicht ... 263
4.1. Inhalt und Konkretisierung der Rechenschaftspflicht ... 264
4.2. Zwei Ebenen der Rechenschaft in ZaPuK ... 265
4.3. Verzeichnis von Verarbeitungstätigkeiten ... 266
4.4. Datenschutz-Folgenabschätzung ... 266
4.5. Nachweis der Wirksamkeit der Sicherheitsmaßnahmen ... 268
4.6. Technische Nachweisfähigkeit und ihr Verhältnis zur Datenminimierung. 268
4.7. Rechenschaft im verteilten Betrieb ... 269
4.8. Folgerungen für die Architektur von ZaPuK ... 270
5. Datenschutz durch Technikgestaltung (Art. 25 DSGVO) ... 271
5.1. Inhalt und Regelungsgehalt des Art. 25 DSGVO ... 272
5.2. Adressat der Pflicht und Bedeutung für die zentrale Entwicklung ... 274
5.3. Datenschutz durch Technikgestaltung in der ZaPuK-Architektur (Art. 25 Abs. 1 DSGVO) ... 275
5.4. Datenschutzfreundliche Voreinstellungen in der ZaPuK-Architektur (Art. 25 Abs. 2 DSGVO) ... 277
5.5. Technikgestaltung im Anwendungsbereich der JI-Richtlinie ... 278
5.6. Nachweis durch Zertifizierung ... 279

5.7. Folgerungen für die Architektur von ZaPuK 279
IV. IT-Sicherheitsrecht 281
1. Anwendbarer Rahmen und Prüfungsmaßstab 282
2. IT-Sicherheit im Portalverbund (§ 5 OZG, ITSiV-PV) 283
3. Cybersicherheitsrecht des Bundes (BSIG in der NIS-2-Fassung) 285
3.1. Anwendungsbereich 286
3.2. Risikomanagementmaßnahmen 287
3.3. Telekommunikations- und vertrauensdiensterechtliche Sonderregime 288
3.4. Föderale Umsetzung, Umsetzungslücken und Durchsetzung 289
3.5. Folgerungen für die Architektur von ZaPuK 290
V. TK-Recht 292
1. Anwendbarer Rahmen und Prüfungsmaßstab 293
1.1. Einordnung des ZaPuK-Postfachs als Telekommunikationsdienst 294
1.2. Einordnung als digitaler Dienst und Doppelnatur 296
2. Folgen der Einordnung als Telekommunikationsdienst 297
2.1. Fernmeldegeheimnis und Schutz der Kommunikationsbeziehung 297
2.2. Verkehrsdaten und Störungsdaten 298
2.3. Nachrichtenübermittlung mit Zwischenspeicherung 298
2.4. Sicherheitspflichten nach dem TKG, ihr Adressatenkreis und das Verhältnis zum BSIG 299
2.4.1. Die abgestuften Pflichten des § 165 TKG 300
2.4.2. Kern der strengeren Pflichten nach den Absätzen 2 ff. 301
2.4.3. Was für ZaPuK von vornherein ausscheidet 303
2.4.4. Anwendung auf die Betriebsmodelle der Zielarchitektur 303
2.4.5. Verhältnis zum BSIG und Lücke in der Verweiskette 305
2.5. Mitwirkung bei der Telekommunikationsüberwachung und Ende-zu-Ende-Verschlüsselung 305
3. Zusätzlich technische Vorkehrungen bei digitalen Diensten (§ 19 TDDDG) 307
3.1. Gegenstand und Adressat der Pflicht 308

3.2. Anwendbarkeit des § 19 Abs. 2 TDDDG neben der DSGVO 309
3.3. Reichweite: kein Anwendungsgegenstand innerhalb des Postfachzugangs 309
3.4. Grenzen des technisch Möglichen und Zumutbaren 311
3.5. Kein verbleibender Handlungsbedarf 311
3.6. Folgerungen für die Architektur von ZaPuK 312
4. Verhältnis zur DSGVO 313
5. Folgerungen für die Architektur von ZaPuK 314
VI. Einzelfragen zum Elektronischen Rechtsverkehr 317
1. Governance im Bereich Justiz 317
2. Sicherungsniveau von Zugangsnachweisen im elektronischen Rechtsverkehr (fortgeschrittene versus qualifizierte Signatur/Zeitstempel/Siegel) 318
2.1. Der prozessrechtliche Mindeststandard 320
2.1.1. Einreichung an das Gericht 320
2.1.2. Zustellung durch das Gericht an nicht berufsmäßig Beteiligte 321
2.1.3. Keine ergänzenden Vorgaben in der ERVV 322
2.1.4. Beweiskraft im Rahmen freier Beweiswürdigung 322
2.2. Die Bereitstellungsbestätigung nach ADR-0018 als Zugangsnachweis 323
2.2.1. Der jeweils geschuldete Beweis 323
2.2.2. Wirkung der einzelnen Nachweiselemente 324
2.2.3. Die Rollenverteilung als beweiswerterhöhendes Element 325
2.2.4. Grenzen und Einführung in den Prozess 325
2.3. Beweiserleichterungen/Vermutungen 326
2.3.1. Öffentliche elektronische Dokumente – Beweiskraft öffentlicher Urkunden 326
2.3.2. Öffentliche elektronische Dokumente – Echtheitsvermutung bei QES 327
2.3.3. Qualifizierte elektronische Zeitstempel – Vermutung der Richtigkeit 327

2.3.4. Qualifizierter Zustelldienst – Vermutungen gem. Art. 43 Abs. 2 eIDAS-VO 328
2.4. Trennung von Siegelniveau und Anbieterstatus 328
2.5. Folgerungen für die Architektur von ZaPuK 330
3. Formwirksame Einreichung im elektronischen Rechtsverkehr – ZaPuK als sicherer Übermittlungsweg 332
3.1. Der Regelungsrahmen: zwei gleichrangige Wege 333
3.2. Der einschlägige Übermittlungsweg für ZaPuK 334
3.3. Die Bindung von Absenderidentität und Postfach 336
3.3.1. Protokollstandard 336
3.3.2. Feststellung der Identität 336
3.3.3. Authentisierung beim Versand 337
3.3.4. Feststellbarkeit des Versands 337
3.3.5. Ergänzende Anforderungen 338
3.4. Einfache Signatur bleibt zwingend 338
3.5. Wo eine qualifizierte Signatur gleichwohl erforderlich bleibt 340
3.6. Formwirksamkeit und Beweiskraft fallen auseinander 341
3.7. Rechtsänderungsbedarf 341
3.8. Folgerungen für die Architektur von ZaPuK 342
4. Lesebestätigung als elektronisches Empfangsbekenntnis (§ 173 Abs. 3 ZPO) 344
4.1. Wann ein Empfangsbekenntnis verlangt wird 345
4.2. Voluntatives Element: keine automatisierbare Quittung 347
4.3. Form: strukturierter Datensatz und Rücklauf an das Gericht 348
4.4. Identifizierbarkeit, Signatur und Vertrauensniveau 348
4.5. Beweiskraft und Folgen des Ausbleibens 350
4.6. Übertragbarkeit auf die behördliche Zustellung 351
4.7. Folgerungen für die Architektur von ZaPuK 351
5. Zulassung zum elektronischen Rechtsverkehr und Vereinbarkeit mit dem risikobasierten Anschlussverfahren 353

5.1. Kein Zulassungsverfahren für den Übermittlungsweg ... 354
5.2. § 7 ERVV trägt für den ZaPuK-Weg nicht ... 354
5.3. Unzulänglichkeit der risikobasierten Zusicherung für den ERV ... 355
5.4. Empfehlungen für die Architektur von ZaPuK ... 355
VII. Weitere Einzelfragen ... 357
1. Rechtsfolgen unzustellbarer oder fehlerhaft verschlüsselter Nachrichten ... 357
1.1. Abhängigkeit vom Bekanntgabemodell ... 357
1.1.1. Elektronische Übermittlung mit Fiktion ... 358
1.1.2. Bereitstellung zum Abruf über ein Postfach ... 359
1.2. Zusammenfassende Bewertung der Fehlerfolgen ... 360
1.3. eIDAS als Instrument der Fehlervermeidung und Vermutungswirkung ... 360
1.4. Folgerungen für die Architektur von ZaPuK ... 361
2. Fortlaufende Bereitstellungspflicht nach Abruf ... 362
2.1. Ausgangspunkt: Funktion des Postfachs ... 362
2.2. Verwaltungsverfahrensrecht: Der jeweilige Vorgang/Zeitpunkt ist maßgeblich ... 363
2.3. Dauerhafte Sicherung liegt in der behördlichen Sphäre (Akten- und Archivrecht) ... 363
2.4. Datenschutzrechtliche Grenzen einer Dauervorhaltung ... 364
2.5. Telekommunikations-/Verkehrsdatenrecht ... 364
2.6. Punktuelle Mindestvorhaltungspflichten als Referenzmodell (De-Mail-Gesetz) ... 365
2.7. Folgerungen für die Architektur von ZaPuK ... 365
3. Anschlussbedingungen und Föderationskontrolle ... 366
3.1. Ansatz von ZaPuK ... 367
3.2. Rechtsnatur ... 368
3.2.1. Anschlussbedingungen als vertragliche Regelung und AGB ... 368
3.2.2. Vergleich: Anschlussbedingungen für das Verbindungsnetz ... 370
3.2.3. Durchsetzung ohne Zulassungsverfahren ... 371

3.2.4. Ausschlussverfahren ... 372
3.2.5. Haftung und Sanktionen ... 372
3.2.6. Verbleibende Unterschiede ... 373
3.3. Weitere Vergleichsmodelle ... 373
3.4. Untergesetzliche und verordnungsrechtliche Verbindlichkeit ... 374
3.5. Funktion und Grenzen ... 375
3.6. Zu regelnde Punkte ... 376
3.7. Empfehlungen und Ableitungen für die Architektur ... 377
E. Möglichkeiten und Grenzen des IT-StV (Ergänzende Stellungnahme vom 19.10.2026) ... 381
I. Einleitung und Fragestellung ... 381
II. Möglichkeiten: ZaPuK als Produkt des IT-Planungsrats ... 381
III. Grenzen ... 384
1. Verbindlichkeit ... 384
2. Perspektivische Einbeziehung der Justiz ... 384
3. Grenzen der Flexibilität bei der Finanzierung von ZaPuK als Produkt des IT-PLR ... 385
4. Governance des ZaPuK-Kommunikationsverbunds ... 389
5. Weiterhin weitere gesetzliche Regelungen erforderlich ... 390
IV. Mehrwert eines eigenständigen Staatsvertrags bzw. ergänzender staatsvertraglicher Regelungen ... 390

A. Sachverhalt

I. ZaPuK - Hintergrund und Kontext des Vorhabens

Mit dem Beschluss B-2024/28-IT des IT-Planungsrates wurde das Föderale IT-Architekturboard durch den IT-Planungsrat mit der Ausarbeitung einer Zielarchitektur zur Konsolidierung von Postfach- und assoziierten Kommunikationslösungen zu Bürgern, Unternehmen und Organisationen in der föderalen IT-Landschaft beauftragt. In einer ersten Projektphase wurde eine initiale Konzeption dieser Zielarchitektur für Postfach- und Kommunikationslösungen („**ZaPuK**") erarbeitet[1]. Mit dem Beschluss B-2025/28-IT des IT-Planungsrates beauftragte der IT-Planungsrat auf dieser Basis die Föderale IT-Kooperation AöR („**FITKO**") mit Phase 2 der Umsetzung einschließlich u.a. der Fortschreibung und Validierung der Zielarchitektur sowie der Erstellung der Transitions- und Migrationsplanung. Teil des Auftrags an die FITKO für diese Phase 2 war zudem auch die im vorliegenden Gutachten adressierte Frage, auf welcher Rechtsgrundlage der gemeinschaftliche Betrieb der föderalen Postfach- und Kommunikationsinfrastruktur basieren wird. Mit Beschluss B-2026/18-IT des IT-Planungsrates vom 17. Juni 2026 hat der IT-Planungsrat nunmehr ZaPuK als eine der fünf Basiskomponenten des **D-Stacks** anerkannt, für die „der Bund […] mit Unterstützung der FITKO […] die fachliche Verantwortung" trägt, und für die die Länder nach Ziffer 5 des Beschlusses B-2026/18-IT des IT-Planungsrates „verbindlich die Anbindung und Flächendeckung […] sicher[stellen] und […] sich zur Nutzung" verpflichten. Die Konzeptionierung von ZaPuK soll einschließlich Betriebs- und Finanzierungsmodell spätestens bis zur 52. Sitzung des IT-Planungsrates erfolgen.

ZaPuK ist darüber hinaus Teil der **Föderalen Modernisierungsagenda**, die dazu beitragen soll, Deutschland schneller, digitaler und handlungsfähiger zu machen. Maßnahme 207 hält konkret fest, dass im Rahmen von ZaPuK „die Vorschriften für die digitale Bekanntgabe und Zustellungen für Verwaltungsakte zu föderalen Postfachlösungen (Deutschland-ID i.S.d. § 12 Abs. 1 OZG, MUK etc.)" harmonisiert werden sollen. Darüber hinaus steht das ZaPuK-Vorhaben in engem

[1] Föderale Zielarchitektur für Postfach- und Kommunikationslösungen, Zukunftsweisende föderale Infrastruktur für die Kommunikation zwischen Privatpersonen, privaten Organisationen und öffentlichen Stellen, Überblick und Handlungsempfehlung, Version: 1.0, Stand: 13.05.2025, sowie das Begleitdokument: 02_Konzept_Zielarchitektur.

Zusammenhang zu weiteren Maßnahmen der Föderalen Modernisierungsagenda: Maßnahme 208 zielt auf die Realisierung von vollständig digitalen und medienbruchfreien Verwaltungsabläufen und wird flankiert von Maßnahme 40, welche die grundsätzliche Ersetzung der Schriftform durch Textform und Nutzung einfacher E-Mails zwischen Bürgern und Behörden anstrebt. Letzteres ist auf Bundesebene bereits mit dem Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern durch Ersetzung des § 3a VwVfG mit Wirkung zum 1. Juli 2027 umgesetzt worden[2]; auch die verwaltungsverfahrensrechtlichen Regelungen auf Landesebene werden in absehbarer Zeit angepasst[3]. Maßnahme 205 betrifft die Schaffung des D-Stacks als nationale Technologieplattform und 206 die Integration der EUDI-Wallet in den D-Stack, wobei insbesondere die Verknüpfung mit NOOTS und ZaPuK hervorgehoben wird. Maßnahme 201 schließlich spricht ein weiteres Vorhaben an, das für ZaPuK gegebenenfalls Bedeutung erlangen kann: „Bund und Länder streben eine zeitnahe Änderung von Artikel 91c GG an, damit der Bund digitale Verfahren und Standards regeln und IT-Systeme errichten, betreiben und für die Mitnutzung durch die Landesebene zur Verfügung stellen kann."

II. ZaPuK – Wesentliche Bestandteile und Eckpunkte der Zielarchitektur

Das Zielbild von ZaPuK umfasst eine einheitliche föderale Kommunikationsinfrastruktur, über die Privatpersonen, Organisationen und öffentliche Stellen sicher und vertraulich kommunizieren. Umgesetzt werden soll dies durch eine modulare, föderierte Client-Server-Architektur zur sicheren, Ende-zu-Ende-verschlüsselten („**E2EE**") Kommunikation, die im Einklang mit den Vorgaben des D-Stacks auf offenen Standards basiert sowie einen Zero-Trust-Ansatz verfolgt. Als Kommunikationsstandard für die Nachrichtenübermittlung ist der Matrix-Standard der Matrix Foundation vorgesehen. Wesentliche Bestandteile von ZaPuK sind die zentral bereitgestellten Postfach-Backends und Standard-Postfachzugänge; daneben besteht für Organisationen und Unternehmen die Möglichkeit, auch dezentrale eigene Backends zu betreiben.

Eine detaillierte Beschreibung des aktuellen Stands der fortgeschriebenen Zielarchitektur kann der Unterlage „Föderale Zielarchitektur für Postfach- und Kommunikationslösungen,

[2] Veröffentlicht im BGBl. I Nr. 199 vom 9. Juli 2026.

[3] Vgl. z.B. Gesetzentwurf der Landesregierung - Drittes Gesetz zur Entlastung von Bürgern und Wirtschaft in NRW, LT-Drs. 18/20446 vom 7. Juli 2026.

Zielarchitektur (Version 1.1), Bauplan einer modernen Kommunikationsinfrastruktur für Privatpersonen, private Organisationen und öffentliche Stellen“ vom 8. September 2026 (kurz „**ZaPuK-Konzept**“ oder „**das Konzept**“ oder „**Architekturkonzept**“) sowie den in Form von Architectural Decision Records („**ADRs**“) dokumentierten Architekturentscheidungen entnommen werden.

Kurz zusammengefasst können danach die folgenden Eckpunkte der Zielarchitektur hervorgehoben werden:

- **Architekturziele**: ZaPuK verfolgt primär die folgenden fünf Ziele: Abbau von Hürden für den Anschluss; Förderung eines wirtschaftlichen Betriebs durch Konsolidierung; Förderung von Ende-zu-Ende-Sicherheit; Verbesserung der Nutzer:innenerfahrung; Ermöglichung einer zukunftsfähigen Weiterentwicklung auf dem Stand der Technik
- **Integration in den D-Stack und perspektivische Anbindung an europäische Lösungen**: Die Zielarchitektur ist so zu gestalten, dass sie sich als ein abgegrenzter Bestandteil nahtlos in die Deutschland-Architektur einpasst sowie Aspekte der europäischen Interoperabilität berücksichtigt.
- **Zentrale Matrix-Backends**: Zentrale Infrastrukturkomponenten der Architektur sind zum einen ein zentrales Postfach-Backend für Privatpersonen und zum anderen zentrale Backends für Organisationen, verteilt auf drei Homeserver für private Organisationen, öffentliche Stellen und Organisationen der Justiz. Um soweit wie möglich die Entstehung von sensiblen Metadaten zu vermeiden, ist eine Separierung des Betriebs der zentralen Backends für Organisationen einerseits (durch FIT Connect) sowie des zentralen Backends für Privatpersonen andererseits (durch den Bund) vorgesehen.
- Organisationen können anstelle der zentralen Backends eigene **dezentrale Backends** nutzen.
- Ergänzt werden die Backend-Komponenten insbesondere durch ein **Self-Service-portal** und ein **Adressregister** für öffentliche Stellen und private Organisationen und

Unternehmen. Zur Adressierung von Privatpersonen werden Pseudonyme verwendet, ein zentrales Adressregister ist für diese nicht vorgesehen.

- **Frontend/Postfachzugänge**: Die im Postfach-Backend verschlüsselt vorliegenden Nachrichten werden über Matrix-Clients (Postfachzugänge) von den Nutzenden abgerufen. Ein zentraler Postfachzugang für Privatpersonen und Organisationen soll modular entwickelt werden, um auch eingebettet in andere Verwaltungsfrontends wie Bundesportal oder Deutschland-App eingesetzt werden zu können. Daneben können Dritte auch eigene Postfachzugänge betreiben, über die z.B. die Anbindung von Fachverfahren oder Unternehmensanwendungen an die Infrastruktur erfolgen kann.

- ZaPuK ist als reine Postfachlösung konzipiert – die noch im Onlinezugangsgesetz (OZG) vorgesehene Kopplung an ein Nutzerkonto entfällt. Zur **Anmeldung und Authentifizierung der Nutzenden** greift ZaPuK jedoch auf die vorhandenen Lösungen zurück: Privatpersonen authentifizieren sich über BundID, eID und perspektivisch die EUDI-Wallet; für Organisationen erfolgt die Authentifizierung über das Organisationskonto („Mein Unternehmenskonto“) und perspektivisch die European Business Wallet.

B. Prüfauftrag

Gegenstand dieses Gutachtens ist die rechtliche Bewertung der Machbarkeit sowie der Ausgestaltung einer konsolidierten, föderal einheitlichen Postfach- und Kommunikationsarchitektur für öffentliche Stellen in Deutschland auf Grundlage der Zielarchitektur Postfach und Kommunikationslösungen. Die Zielarchitektur wird dabei grundsätzlich in der Gestalt betrachtet und rechtlich bewertet, die sie im Rahmen des ZaPuK-Konzepts Version 1.1 mit Stand vom 8. September 2026 gefunden hat.

Im Fokus der Untersuchung steht zunächst die Frage der Umsetzbarkeit vor dem Hintergrund der verfassungsrechtlichen Kompetenzordnung innerhalb des föderalen Gefüges der Bundesrepublik Deutschland. Die Begutachtung umfasst die Identifikation und Prüfung potenziell einschlägiger Rechtsgrundlagen für die Errichtung und den Betrieb von ZaPuK, ihrer

dogmatischen Reichweite und Grenzen im Einzelnen sowie ihrer Auswirkungen auf die Finanzierung des Vorhabens (Abschnitt D.I.).

Im Anschluss werden verwaltungsverfahrensrechtliche Rahmenbedingungen in den Blick genommen (Abschnitt D.II.), soweit sie für die rechtliche Bewertung der in Betracht kommenden Architektur von Bedeutung sein können. Der Fokus liegt insoweit auf den auch im Rahmen der Föderalen Modernisierungsagenda adressierten für ZaPuK relevanten Vorschriften für die digitale Bekanntgabe und Zustellung von Verwaltungsakten.

Darüber hinaus ist die Architektur von ZaPuK auf diejenigen Rahmenbedingungen abzustimmen, die sich aus dem Datenschutzrecht (Abschnitt D.III.), dem IT-Sicherheitsrecht (Abschnitt D.IV.) und dem Telekommunikationsrecht (Abschnitt D.V.) ableiten.

Schließlich werden in den Abschnitten D.VI. und D.VII. sektorspezifische Besonderheiten im Bereich der Justiz sowie weitere Einzelfragen behandelt, die sich aus der Konzeption von ZaPuK ergeben.

Grundlage der rechtlichen Untersuchungen ist die aktuell geltende Rechtslage, wobei solche rechtlichen Entwicklungen in die Betrachtung mit einbezogen werden, die bereits konkret absehbar sind.

Davon ausgehend wird jeweils herausgearbeitet, welche rechtlichen Regelungen für die Umsetzung einer zentralen Postfach- und Kommunikationsstruktur in Gestalt von ZaPuK zu berücksichtigen sind und welche konkreten Folgerungen sich daraus für die Konzeption und Umsetzung für ZaPuK ergeben. Darüber hinaus werden Empfehlungen zur Anpassung der geltenden Rechtslage ausgesprochen, soweit diese vor dem Hintergrund der anwendbaren verfassungsrechtlichen, verwaltungsverfahrensrechtlichen, datenschutzrechtlichen, IT-sicherheitsrechtlichen oder TK-rechtlichen Regelungen für die Umsetzung von ZaPuK notwendig oder sachgerecht erscheinen.

C. Lesehilfen: Folgerungen für ZaPuK und Empfehlungen für Rechtsänderungen

Die sich aus den anwendbaren rechtlichen Regelungen jeweils ergebenden **konkreten Folgerungen für die Konzeption und Umsetzung von ZaPuK** sind im Gutachten an den folgenden Stellen zu finden:

Inhaltlicher Kontext	Kurzzusammenfassung der Folgerungen für ZaPuK bzw. Schlagwörter zur Orientierung	Zu finden in Abschnitt:
Konnexitätsgrundsatz	Die Finanzierungsverantwortung folgt der Verwaltungszuständigkeit, soweit nicht das GG Abweichungen zulässt – diese Folgen sind bei der Ausgestaltung von ZaPuK stets mitzudenken.	**D.I.1.3.1**
Untersuchung potenzieller verfassungsrechtlicher Rechtsgrundlagen für das Vorhaben	**Einzelne verfassungsrechtliche Regelungen kommen potenziell als Rechtsgrundlage in Betracht, sind aber – jeweils isoliert betrachtet – unzureichend, um die für ZaPuK angestrebte Architektur zufriedenstellend umzusetzen.** Im Einzelnen: ➢ Art. 84, 85, 86 GG: nur Ausführung von Bundesgesetzen, Regelungsmöglichkeiten zur Finanzierung nicht zufriedenstellend ➢ Art. 91c Abs. 4 GG eignet sich nicht als Rechtsgrundlage, begrenzt auf internen Austausch ➢ Art. 91c Abs. 5 GG: Bundeskompetenz für gesetzl. Regelungen, ermöglicht iVm Art. 87 Abs. 3 GG auch bundeseigene Verwaltung und Finanzierung, soweit gewünscht; für Justiz Rückgriff auf Art. 74 GG erforderlich. ➢ Art. 91c Abs. 1, 2 GG erlaubt Zusammenwirken von Bund und Ländern, auch z.B. Betrieb durch die FITKO; per Staatsvertrag – separat oder auch als Teil eines D-Stack-StV – können Kooperationsbeiträge und Verantwortlichkeiten der Beteiligten klar	**D.I.2.1.4** **D.I.2.2.1** **D.I.2.2.2.c)** **D.I.2.2.3.d)**

	definiert und Finanzierungsanteile sachgerecht zugeordnet werden. ➢ Art. 108 Abs. 4, Abs. 1 ff. GG ermöglicht grundsätzlich Erstreckung von ZaPuK auch auf die Steuerverwaltung, durch Bundesgesetz mit Zustimmung des Bundesrates	**D.I.2.2.4**
Untersuchung potenzieller verfassungsrechtlicher Rechtsgrundlagen für das Vorhaben	**Lösung: Herleitung der rechtlichen Machbarkeit des Gesamtvorhabens durch Zusammenführung der o.g. Gesetzgebungs- und Verwaltungskompetenzen.** Ermöglicht zentrale Finanzierung und Bereitstellung erheblicher Teile der Infrastruktur, zugleich aber die angestrebte Trennung der Betriebsverantwortung für die zentralen Backends zwischen Bund und FITKO; StaatsV erlaubt klare Regelung von Vollzugsverantwortlichkeiten und sachgerechte Zuordnung von Finanzierungsanteilen.	**D.I.2.3**
Verfassungsrechtliche Rechtsgrundlagen für das Vorhaben	Vorzugswürdig mit Blick auf Rechtsklarheit und -sicherheit wäre eine **Erweiterung des Art. 91c GG** um eine Ermächtigungsgrundlage, auf deren Basis der Bund IT-Systeme errichten, betreiben und für die Mitnutzung durch die Landesebene zur Verfügung stellen kann (vgl. Föderale Modernisierungsagenda, Maßnahme 201).	**D.I.3**
Verwaltungsverfahrensrechtliche Fragen	Elektronische Kommunikation über ZaPuK setzt zumindest konkludente Zugangseröffnung voraus: bei Organisationen genügt Registrierung im Self-Service-Portal; für Privatpersonen idR durch Antragstellung; auch bei Vorliegen einer Adresse aus früherem Vorgang oder nach Authentisierung zulässig.	**D.II.1.5**
Digitale Bekanntgabe	Bei Verwendung dezentraler Backends durch Organisationen kann eine Bekanntgabe in der	**D.II.2.2.1.c)**

von Verwaltungsakten	Übermittlungsvariante (u.a. § 41 Abs. 2 Satz 2 VwVfG) erfolgen; Eingang in den Machtbereich des Empfängers wird durch automatische serverseitige Bereitstellungsbestätigung belegt	
Digitale Bekanntgabe von Verwaltungsakten	Die von ZaPuK vorgesehenen Systeme zur Authentisierung/Authentifizierung der abrufberechtigten Person bei Bereitstellung zum Abruf folgen grds. den bestehenden und absehbaren gesetzlichen Lösungen.	**D.II.2.2.2.a)bb)(4)**
Digitale Bekanntgabe von Verwaltungsakten / Bekanntgabefiktionen	ZaPuK sollte die folgenden Vorgänge und entspr. Zeitpunkte erfassen bzw. nachweisen können: **Abruf** des Verwaltungsakts, **Bereitstellung** und Bereitstellungszeitpunkt im Postfach, Absendung und – soweit möglich – **Zugang der Benachrichtigung** über die Bereitstellung des Verwaltungsakts beim Beteiligten Umsetzung in ZaPuK grds. durch automatische serverseitige Bereitstellungsbestätigungen sowie automatische clientseitige Abrufbestätigungen; Empfehlung: Vermeidung oder revisionssichere Dokumentation von Verschlüsselungsfehlern	**D.II.2.2.2.b)ff)** Vgl. auch: **D.II.2.2.2.b)aa),** **D.II.2.2.2.b)bb),** **D.II.2.2.2.b)cc),** **D.II.2.2.2.b)dd),** **D.II.2.2.2.b)ee)**
Digitale Zustellung von Dokumenten	Zustellung erfordert qualifizierte elektronische Signatur – ZaPuK erlaubt unveränderte Übermittlung von Dokumenten mit QES, aber stellt Signatur nicht selbst bereit; aktive Lesebestätigung, erweiterbar zum elektronischen Empfangsbekenntnis unter Wahrung der E2EE-Konformität, ist vorgesehen; EB sollte Empfänger eigenständige Eintragung des Zustelldatums erlauben	**D.II.2.3.4**
Schriftformersatz/	Soweit QES erforderlich, erlaubt ZaPuK unveränderte Übermittlung von Dokumenten mit QES (s.o.)	**D.II.3.2, D.II.3.3**

elektron. Form	Anforderungen an "sicheren Übermittlungsweg" je nach gesetzl. Entwicklung	
Datenschutz	Anwendbares Datenschutzrecht: DSGVO sowie weitere nationale Regelungen, angesichts einer Vielzahl von Schutzregimen Ausrichtung an höchstem Schutzniveau; Datenverarbeitung und Rollen in ZaPuK	**D.III.1.1.5, D.III.1.2.7, D.III.1.3.3**
Datenschutz	Datenschutzrechtliche Rollen, datenschutzrechtliche Verantwortung insb. von Backend-Betreibern	**D.III.2.3**
Grundsätze des Datenschutzes	Rechtmäßigkeitsgrundsatz Zweckbindung Datenminimierung Richtigkeit Speicherbegrenzung (Löschung und Archivierung, Logdaten)	**D.III.3.1.7** **D.III.3.2.5** **D.III.3.3.4** **D.III.3.4.3** **D.III.3.5.1.f), D.III.3.5.2.f)**
Datensicherheit	Integrität Vertraulichkeit durch Verschlüsselung: Verbindlichkeit, Reichweite und Endpunkte der Ende-zu-Ende-Verschlüsselung, serverseitige Verarbeitung (Malware-Prüfung), Archivierung und Stellvertretung, Schlüsselmanagement und -wiederherstellung Vertraulichkeit der Kommunikationsbeziehung (Metadatenschutz)	**D.III.3.6.1.e)** **D.III.3.6.2.a)ff), D.III.3.6.2.b)ff), D.III.3.6.2.c)gg), D.III.3.6.2.d)dd), D.III.3.6.2.e)ff)** **D.III.3.6.3.d)**
Datenschutz	Rechenschaftspflicht der verantwortlichen Stelle bzgl. Einhaltung der Verarbeitungsgrundsätze; ZaPuK-Infrastruktur muss den Nachweis ermöglichen und dokumentierbar machen	**D.III.4.8**
Datenschutz	Durch Technikgestaltung: Datenschutzeigenschaften sollten in die zentral bereitgestellten Bausteine	**D.III.5.7**

	eingebaut, dokumentiert und über die Anschlussbedingungen verbindlich gemacht werden; Ausrichtung der noch offenen Entwurfsentscheidungen am Maßstab des Art. 25 DSGVO	
IT-Sicherheitsrecht	ITSiV-PV gilt für zentrale Postfach-Komponenten; BSIG betreiberbezogen einschlägig	**D.IV.3.5**
TK-Recht	Einordnung des ZaPuK-Postfachs als nummernunabhängiger interpersoneller Telekommunikationsdienst; Einordnung als digitaler Dienst; Geltung des Fernmeldegeheimnisses; strenge Zweckbindung und Erfordernis der Löschung der Verkehrsdaten; Sicherheitspflichten; Mitwirkungspflichten bei der Telekommunikationsüberwachung	**D.V.5**
ERV	Sicherungsniveau von Zugangsnachweisen im elektronischen Rechtsverkehr Empfehlungen: Serversignatur der Bereitstellungsbestätigung als fortgeschrittenes elektronisches Siegel mit Zertifikatsbindung an den Betreiber; verordnungsrechtl. Festlegung der Form der Bereitstellungsbestätigung; qualifizierter elektronischer Zeitstempel; Clients müssten die gerichtsseitige Eingangsbestätigung nach § 130a Abs. 5 Satz 2 ZPO entgegennehmen	**D.VI.2.5**
ERV	Formwirksame Einreichung im ERV	**D.VI.3.8**
ERV	Lesebestätigung als elektronisches Empfangsbekenntnis, Postfachzugänge sollten die aus der Nutzung folgende Kontrollobliegenheit sichtbar machen	**D.VI.4.7**
ERV	Zulassung zum ERV erforderte eine Reihe Anpassungen; ggf. gesetzl. Regelung	**D.VI.5.4**

Digitale Bekanntgabe	Folgen unzustellbarer oder fehlerhaft verschlüsselter Nachrichten; Empfehlung: Vermeidung oder revisionssichere Dokumentation von Verschlüsselungsfehlern	**D.VII.1.4**
Vorhaltung elektronischer Nachrichten	Definierte, begründete Vorhaltefristen für ZaPuK als Gestaltungsentscheidung; keine gesetzliche Dauervorhaltepflicht; architektonische Gewährleistung der Speicherbarkeit	**D.VII.2.7**
Anschlussbedingungen	In den Anschlussbedingungen sind bestimmte Punkte zu regeln; außerdem ergeben sich Empfehlungen für die Ausgestaltung der Architektur; dreistufiger rechtlicher Rahmen zu empfehlen (s. nachfolgende Tabelle)	**D.VII.3.6, D.VII.3.7**

Tabelle 1: Folgerungen für ZaPuK

Die folgenden **Anregungen und Empfehlungen für Anpassungen an der geltenden Rechtslage** sind in den verschiedenen Abschnitten des Gutachtens enthalten:

Inhaltlicher Kontext	Empfehlung/Anregung	Zu finden in Abschnitt:
Verfassungsrechtliche Grundlage	Erweiterung des Art. 91c GG um einheitliche Ermächtigungsgrundlage	**D.I.3**
Digitale Bekanntgabe	Regelung der zulässigen Mittel für die Identifizierung/ Authentifizierung analog der Neufassung des § 3 OZG gem. Art. 2 DIdG-E bzw. als Ergänzung zu § 3 OZG	**D.II.2.2.2.a)bb)(4)**
Digitale Bekanntgabe	Sofern § 9 OZG auf ZaPuK-Postfächer Anwendung finden soll: Anknüpfung an einheitliche ZaPuK-	**D.II.2.2.2.b)bb)**

	Abrufumgebung, **Entkopplung Postfach und Nutzerkonto**	
Digitale Bekanntgabe	Entkopplung von Postfach und Nutzerkonto auch in § 122a Abs. 5 AO erforderlich	**D.II.2.2.2.b)cc)**
Digitale Bekanntgabe	Harmonisierung der Regelungen zur elektronischen Bekanntgabe von Verwaltungsakten: bereichsübergreifende Anknüpfung an ein einheitliches Bekanntgabeereignis (z.B. Bereitstellung im Postfach) unter Beibehaltung einer Fiktionsregelung, Regelung an zentraler Stelle im Verwaltungsverfahrensrecht mit Verweisen im Fachrecht	**D.II.2.2.2.b)gg)**
Elektronische Form/ sichere Übermittlungswege	Anerkennung von ZaPuK als „sicherer Übermittlungsweg" (nach vorauss. Rechtslage ab 1.7.27 durch Rechtsverordnung gem. § 3c Abs. 2 VwVfG n.F.) Erstreckung des Anwendungsbereichs der §§ 3b Satz 1 Nr. 3 und 3c Abs. 1 VwVfG n.F. auch auf die behördenseitige Übermittlung elektronischer Dokumente (jetziger Wortlaut: „einreicht")	**D.II.3.2, D.II.3.3**
Datenschutzrecht	Nach Vorbild des § 8 OZG: Prüfung einer spezialgesetzlichen Verankerung für bereichsübergreifende Verarbeitungen; ausdrückliche Zuweisung von Verantwortungen bei verteiltem Betrieb; spezialgesetzliche Grundlage für die	**D.III.1.2.7,** **D.III.2.3,** **D.III.3.1.5,** **D.III.3.2.3**

	Infrastruktur- und Metadatenverarbeitung; ausdrückliche Bindung eines Dritten, an den Daten aus dem Postfach übermittelt werden, an den Übermittlungszweck	
Grundsätze des Datenschutzes	Verbindliche Vorgabe der Ende-zu-Ende-Verschlüsselung, durch Verordnung oder gesetzlich	**D.III.3.6.2.a)ee), D.III.3.6.2.a)ff)**
ERV – Sicherungsniveau von Zugangsnachweisen	Für Urkundenbeweiskraft: rechtliche Festlegung der Form der Bereitstellungsbestätigung empfohlen, z.B. durch eine Regelung nach § 5 oder § 6 OZG, die Verordnung nach § 3c Abs. 2 VwVfG n.F. oder eine spezialgesetzliche Grundlage.	**D.VI.2.5**
ERV – Formwirksame Einreichung	Ausdrückliche Festlegung von ZaPuK durch Rechtsverordnung nach § 130a Abs. 4 Satz 1 Nr. 5 ZPO als bundeseinheitlich sicheren Übermittlungsweg. Anpassung von § 130a Abs. 4 Satz 1 Nr. 4 ZPO, wenn Kopplung von Postfach und Nutzerkonto (§ 2 Abs. 7 Satz 2 OZG) im Zuge der empfohlenen OZG-Anpassung entfällt. Parallel dazu § 55a Abs. 4 Satz 1 Nr. 4 VwGO, § 46c ArbGG, § 65a SGG, § 52a FGO und § 32a StPO. Anpassungen an: Katalog der Identifizierungsmittel in § 11 Abs. 2 Satz 2 ERVV, Katalog der Authentisierungsmittel in § 11 Abs. 3 ERVV	**D.VI.3.7**

	Klarstellung durch Bekanntmachung nach § 5 ERVV oder durch Verordnungsänderung dass Matrix OSCI im Sinne des § 13 Abs. 1 Nr. 1 ERVV ersetzt.	
Zulassung zum ERV	Empfohlene Festlegung von ZaPuK als bundeseinheitlicher sicherer Übermittlungsweg durch Rechtsverordnung nach § 30a Abs. 4 Satz 1 Nr. 5 ZPO sollte zugleich genutzt werden, um ein Zulassungsverfahren zum ERV und dessen Rechtsfolgen zu normieren. Damit würde die verbundinterne Zulassung von einer bloß vertraglichen zu einer rechtlich tragenden Entscheidung.	**D.VI.5.4**
Fortlaufende Bereitstellungspflicht nach Abruf	Anregung: ausdrückliche gesetzliche Regelung der Vorhalte-, Export- und Löschmodalitäten des zentralen Postfachs, um Rechtssicherheit für Bekanntgabe-/Zustellwirkungen, Datenschutz und Nutzererwartungen einheitlich herzustellen	**D.VII.2.7**
Anschlussbedingungen	Dreistufiger rechtlicher Rahmen zu empfehlen: Rechtsverordnung nach §§ 5, 6 OZG für Architektur-, Interoperabilitäts- und Sicherheitsvorgaben mit Wirkung gegenüber allen Stellen; Beschluss des IT-Planungsrates nach § 2 IT-StV für die föderale Bindungswirkung dort, wo eine Verordnung nicht trägt; Anschlussvertrag im SSP[4]-Onboarding	**D.VII.3.7**

[4] Self-Service-Portal.

	für die betreiberbezogenen Pflichten, die Haftung und die Föderationskontrolle	

Tabelle 2: Anregungen und Empfehlungen für Rechtsänderungen

D. Rechtliche Würdigung

I. Verfassungsrechtliche Machbarkeit einer föderal einheitlichen Postfach- und Kommunikationsstruktur

Im Folgenden soll zunächst die verfassungsrechtliche Ausgangslage in der Bundesrepublik Deutschland überblickartig dargestellt werden (Abschnitt 1), um im Anschluss untersuchen zu können, welche verfassungsrechtlichen Rechtsgrundlagen für die Realisierung einer einheitlichen föderalen Postfach- und Kommunikationsinfrastruktur auf Basis der Zielarchitektur für Postfach- und Kommunikationslösungen in Betracht kommen (Abschnitt 2). Danach soll ein ggf. vorhandener Bedarf für eine Grundgesetzänderung thematisiert werden (Abschnitt 3).

1. Verfassungsrechtliche Ausgangslage

Die in Abschnitt 2 zu untersuchenden verfassungsrechtlichen Rechtsgrundlagen für ZaPuK sind Teil einer kompetenziellen Verfassungsordnung, aus der sich jeweils Grenzen und Potenziale für die Machbarkeit und Ausgestaltung einer Postfach- und Kommunikationsinfrastruktur ergeben. Die wesentlichen Eckpunkte dieser verfassungsrechtlichen Ausgangslage sind: die föderale Verteilung der Gesetzgebungsbefugnisse (dazu 1.1) und der Verwaltungskompetenzen (dazu 1.2) in der Bundesrepublik Deutschland sowie die dabei zu beachtenden übergeordneten Grundsätze (dazu 1.3). Eine Besonderheit – eine Art Ausreißer – stellt in diesem Zusammenhang Art. 91c GG dar, mit dem das Grundgesetz (GG) eine Sondervorschrift für die Zusammenarbeit zwischen dem Bund und den Ländern für den Bereich der Informationstechnik statuiert (dazu 1.4).

1.1. Ausgangspunkt I: Kompetenzverteilung in der deutschen Gesetzgebung

Ausgangspunkt des staatlichen Kompetenzgefüges in Deutschland ist Art. 30 GG:

> *Die Ausübung der staatlichen Befugnisse und die Erfüllung der staatlichen Aufgaben ist Sache der Länder, soweit dieses Grundgesetz keine andere Regelung trifft oder zuläßt.*

Entsprechend weist Art. 70 Abs. 1 GG den Ländern grundsätzlich das Recht zur Gesetzgebung zu. Dem Bund verleiht das Grundgesetz dagegen nur in den ausdrücklich vorgesehenen Fällen Gesetzgebungskompetenzen, in denen sich dies aus den Katalogen der ausschließlichen Gesetzgebung (Art. 71, 73 GG) und der konkurrierenden Gesetzgebung (Art. 72, 74 GG) ergibt. Darüber hinaus erkennt die verfassungsrechtliche Dogmatik neben den ausdrücklich normierten Zuständigkeiten jedoch auch ungeschriebene Gesetzgebungskompetenzen des Bundes an, namentlich die Annexkompetenz[5], die Kompetenz kraft Sachzusammenhangs[6] sowie die Kompetenz kraft Natur der Sache[7]. Auf Basis einer ungeschriebenen Gesetzgebungszuständigkeit ist es dem Bund nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) allerdings nicht gestattet, die den Ländern vorbehaltene Materie umfassend an sich zu ziehen und zu regeln. Zulässig ist lediglich, diejenigen Einzelregelungen zu treffen, ohne die der Bund die ihm ausdrücklich zugewiesene Kompetenz nicht sinnvoll nutzen könnte. Wann dies der Fall ist, lässt sich nicht generell und abstrakt bestimmen, sondern nur unter Berücksichtigung der Besonderheiten des jeweiligen Regelungsgegenstands.[8]

Eine Kompetenznorm, die es dem Bund ermöglichen würde, die Verwaltungsdigitalisierung in Deutschland umfassend zu regeln, enthält das GG nicht. Allerdings kommt für die

---

5 Die Annex-Kompetenz erstreckt die Gesetzgebungsbefugnisse des Bundesgesetzgebers in Bezug auf bestimmte, ihm ausdrücklich zugewiesene Materien auf die Stadien der Vorbereitung und Durchführung, siehe Degenhart, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 70, Rn. 36.

6 Die Gesetzgebungskompetenz des Bundes kraft Sachzusammenhangs bezieht sich auf Fälle, in denen eine dem Bund zugewiesene Materie sinnvollerweise nicht geregelt werden kann, ohne zugleich eine dem Bundesgesetzgeber nicht ausdrücklich zugewiesene Materie mitzuregeln. Das Übergreifen in diese Materie muss danach unerlässliche Voraussetzung für die Regelung der dem Bund zugewiesenen Materie sein, siehe BVerfG, Urteil vom 30.10.1962 - 2 BvF 2/60, 1-3/61, NJW 1962, 2243 (2246); Beschluss vom 09.07.1969 - 2 BvL 25/64, 2 BvL 26/64, BeckRS 1969, 104923, Rn. 74.

7 Eine Gesetzeskompetenz kraft Natur der Sache wird für solche Gegenstände anerkannt, für die denklogisch nur eine Regelung durch ein Bundesgesetz in Betracht kommt (etwa Bundessymbole oder der Sitz der Bundesregierung), siehe Degenhart, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 70, Rn. 30.

8 BVerfG, Urteil vom 27.10.1998 - 1 BvR 2306–96, 2314–96, 1108–97, 1109–97 u. 1110–97, NJW 1999, 841 (842).

Verwirklichung von ZaPuK eine Reihe verfassungsrechtlicher Rechtsgrundlagen in Betracht, die jeweils an verschiedene Aspekte einer einheitlichen föderalen Postfach- und Kommunikationsinfrastruktur und daher im Einzelnen auf ihre Reichweite und Tragfähigkeit untersucht werden müssen (dazu im Einzelnen Abschnitt 2).

1.2. Ausgangspunkt II: Kompetenzverteilung in der deutschen Verwaltung

1.2.1. Grundsatz: Zuständigkeit der Länder für den Verwaltungsvollzug

Ausgehend von Art. 30 GG obliegt auch der Verwaltungsvollzug in Deutschland grundsätzlich den Ländern. Dies gilt sowohl für die Ausführung des eigenen Landesrechts als auch für den Vollzug von Bundesrecht. In Art. 83 GG wird dies für die Ausführung der Bundesgesetze konkretisiert:

> *Die Länder führen die Bundesgesetze als eigene Angelegenheit aus, soweit dieses Grundgesetz nichts anderes bestimmt oder zuläßt.*

Abweichungen von dieser Grundregel müssen im GG also ausdrücklich verankert sein. Das bedeutet: Der Bund darf Verwaltungsaufgaben nur übernehmen, wenn ihm das GG hierfür eine eigene Verwaltungskompetenz zuweist.[9]

Liegt die Verwaltungskompetenz danach bei den Ländern, bedeutet dies jedoch nicht in jedem Fall, dass diese auch für die Regelung der Einzelheiten des Verwaltungsverfahrens zuständig wären. Vielmehr verbleiben dem Bund nach den Art. 83 ff. GG punktuell Gestaltungsspielräume, soweit die Ausführung von Bundesrecht betroffen ist. Für das von den Ländern ausgeführte Landesrecht gilt dies nicht - diesbezüglich fehlt es an einer Regelungs- und Organisationskompetenz des Bundes.[10]

---

[9] Die Regelungen aus Art. 30 GG und dem VIII. Abschnitt des GG gelten sowohl für die gesetzesakzessorische – also die Ausführung einfachgesetzlicher Bestimmungen betreffende – als auch für die „gesetzesfreie" – nicht im Detail durch einfachgesetzliche Bestimmungen geregelte – Erfüllung von Aufgaben, siehe BVerfG, Urteil vom 28.02.1961 – 2 BvG 1 u. 2/60, NJW 1961, 547 (549); vgl. auch Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 86, Rn. 4.

[10] Schliesky: Verfassungsrechtliche Rahmenbedingungen des E-Government, DÖV 2004, S. 809 (813 f.).

Hinsichtlich der Ausführung von Bundesrecht durch die Länder ist zu differenzieren:

a) Ausführung der Bundesgesetze durch die Länder als eigene Angelegenheit

In den Fällen, in denen die Länder Bundesgesetze **als eigene Angelegenheit** ausführen, obliegt ihnen gemäß Art. 84 Abs. 1 Satz 1 GG grundsätzlich auch die gesetzliche Regelung der Einrichtung der Behörden und des Verwaltungsverfahrens. Sie können darüber entscheiden, wie sie ihre Verwaltung organisieren, welcher Stelle sie welche *Aufgaben* zuweisen und wie sie das Verfahren ausgestalten.[11]

IT-bezogene Vorgaben, wie beispielsweise Vorgaben zur Nutzung von ZaPuK, betreffen in der Regel die sachliche Ausstattung der Behörden und damit die „Behördeneinrichtung".[12] Zugleich können aber auch verfahrensrechtliche Regelungen Anforderungen an die Verwaltungsdigitalisierung beinhalten.[13] Kompetenziell obliegt es den Ländern demnach grundsätzlich, die IT-Infrastruktur für die elektronische Abwicklung ihrer Verwaltungsverfahren zu regeln, zu errichten und zu betreiben.[14]

Allerdings wird in Art. 84 Abs. 1 Sätze 2-6 GG für den Vollzug von Bundesrecht durch die Länder als eigene Angelegenheit auch eine Regelungsbefugnis des Bundes adressiert:

> *[2]Wenn Bundesgesetze etwas anderes bestimmen, können die Länder davon abweichende Regelungen treffen. [3]Hat ein Land eine abweichende Regelung nach Satz 2 getroffen, treten in diesem Land hierauf bezogene spätere bundesgesetzliche Regelungen der Einrichtung der Behörden und des Verwaltungsverfahrens frühestens sechs Monate nach ihrer Verkündung in Kraft, soweit nicht mit Zustimmung des Bundesrates anderes bestimmt ist. [4]Artikel 72 Abs. 3 Satz 3 gilt entsprechend. [5]In Ausnahmefällen kann der Bund wegen eines*

[11] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 84, Rn. 15.
[12] Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Band 3, Art. 83-146, 8. Auflage 2024, Art. 91c, Rn. 5.
[13] Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 84, Rn. 11.
[14] Vgl. Schliesky: Verfassungsrechtliche Rahmenbedingungen des E-Government, DÖV 2004, S. 809 (811 f.), der für den Bereich der bundeseigenen Verwaltung erläutert, dass die Bereitstellung von IT-Basiskomponenten von der „Einrichtung" der Behörden in Art. 86 Satz 2 GG begrifflich gedeckt ist.

besonderen Bedürfnisses nach bundeseinheitlicher Regelung das Verwaltungsverfahren ohne Abweichungsmöglichkeit für die Länder regeln. [6]Diese Gesetze bedürfen der Zustimmung des Bundesrates.

(Hervorhebung hier hinzugefügt)

Da die Ausgestaltung verfahrensrechtlicher und organisatorischer Vorgaben die effektive Umsetzung materieller Regelungsziele maßgeblich beeinflussen kann, erhält der Bundesgesetzgeber in diesem Kontext die Möglichkeit, eigene Regelungen über die Einrichtung der Behörden und das Verwaltungsverfahren zu treffen[15] und insofern auf die Ausgestaltung IT-gestützter Verwaltungsprozesse im Bereich der Länder einzuwirken. Rechtsdogmatisch wird Art. 84 Abs. 1 Satz 2 Halbsatz 1 GG zum Teil als eigenständige Kompetenznorm des Bundes verstanden, die entweder als spezielle Bestimmung den allgemeinen Regelungen der Art. 70 ff. GG im Verwaltungstypus nach Art. 83 GG vorgehe,[16] oder der Sache nach zu dem Bereich der konkurrierenden Gesetzgebung im Sinne des Art. 72 Abs. 1 GG zähle[17]. Nach anderer Auffassung geht die Gesetzgebungskompetenz des Bundes hinsichtlich Organisations- und Verfahrensregeln für den Landesvollzug von Bundesgesetzen bereits mit den sachlichen Gesetzgebungskompetenzen der Art. 70 ff. GG einher.[18]

Art. 84 Abs. 1 Satz 2 Halbsatz 2 GG räumt den Ländern insoweit jedoch ein Abweichungsrecht ein. Abweichend vom Bundesrecht können sie eine eigene gesetzliche Regelung treffen (actus contrarius-Gedanke), die, wie aus dem Verweis in Art. 84 Abs. 1 Satz 4 GG auf Art. 72 Abs. 3 Satz 3 GG folgt, als *lex posterior* zur Unanwendbarkeit der bundesrechtlichen Organisations- oder Verfahrensregelung in dem betreffenden Land führt.[19] Gemäß Art. 84 Abs. 1 Satz 5 und 6

---

15 Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 84, Rn. 16.

16 Ebd., Rn. 17.

17 M. Ronellenfitsch/L. Ronellenfitsch, in BeckOK VwVfG, Bader/Ronellenfitsch, 69. Edition, Stand: 01.10.2025, § 1, Rn. 62.

18 Roth-Isigkeit, Verfassungsrechtliche Möglichkeiten der Aufgabenbündelung im Föderalstaat, Rechtsgutachten im Auftrag des Nationalen Normenkontrollrats (NKR), S. 19.

19 Auf die abweichende landesgesetzliche Regelung bezogene spätere bundesgesetzliche Regelungen treten nach der in Art. 84 Abs. 1 Satz 3 GG vorgesehenen Karenzzeit frühestens sechs Monate nach der Verkündung in Kraft; ein früheres Inkrafttreten ist nur mit Zustimmung des Bundesrates möglich, siehe Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 84, Rn. 35-38.

GG ist es dem Bundesgesetzgeber allerdings gestattet, mit Zustimmung des Bundesrats im Ausnahmefall wegen eines besonderen Bedürfnisses nach bundeseinheitlicher Regelung das *Verwaltungsverfahren* – nicht hingegen die Behördeneinrichtung – ohne Abweichungsmöglichkeit für die Länder zu regeln.[20]

b) Bundesauftragsverwaltung

Neben dem in Art. 83 und 84 GG normierten Regelvollzug durch die Länder als eigene Angelegenheit ist im GG auch die Möglichkeit vorgesehen, dass die Länder Bundesrecht im Rahmen der **Auftragsverwaltung** vollziehen. Auch in diesem Fall bleibt die Einrichtung der Behörden gemäß Art. 85 Abs. 1 GG prinzipiell Ländersache. Die Bundesauftragsverwaltung stellt danach eine Form der Landesverwaltung dar, die im Grundsatz auch die Organisation des verwaltungsmäßigen Vollzugs der Bundesgesetze umfasst.[21] Eine Einschränkung dieser Befugnis erfolgt aber wiederum durch die in Art. 85 Abs. 1 Satz 1, 2. Halbsatz GG adressierte Bundeskompetenz:

> *[1]Führen die Länder die Bundesgesetze im Auftrage des Bundes aus, so bleibt die Einrichtung der Behörden Angelegenheit der Länder, soweit nicht Bundesgesetze mit Zustimmung des Bundesrates etwas anderes bestimmen. [2]Durch Bundesgesetz dürfen Gemeinden und Gemeindeverbänden Aufgaben nicht übertragen werden.*
>
> (Hervorhebung hier hinzugefügt)

Nach einheitlicher Auffassung darf der Bund zudem im Rahmen der Bundesauftragsverwaltung durch die Länder nicht nur die in Art. 85 Abs. 1 Satz 1 GG ausdrücklich erwähnte Einrichtung der Behörden, sondern auch das Verwaltungsverfahren gesetzlich regeln. Begründet wird dies mehrheitlich mit einem „Erst-Recht-Schluss" ausgehend von Art. 84 GG.[22] Anders als für die

[20] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 84, Rn. 40-43.

[21] BVerfG, Urteil vom 22.05.1990 - 2 BvG 1/88, BeckRS 1990, 1414; Winkler, in: Sachs, Grundgesetz, 10. Aufl. 2024, Art. 85, Rn. 9 f.

[22] Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 85, Rn. 12; Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 85, Rn. 15-18.

Regelung der Behördeneinrichtung ist der Bund dabei nicht auf die Zustimmung des Bundesrates angewiesen.[23]

Art. 85 Abs. 2 bis 4 GG gestehen dem Bund im Fall der Bundesauftragsverwaltung darüber hinaus zusätzliche Einwirkungsbefugnisse zu. Diese bestehen aus dem Erlass von Verwaltungsvorschriften, einem Weisungsrecht der obersten Bundesbehörde sowie der Bundesaufsicht, die gemäß Art. 85 Abs. 4 GG die Gesetz- und Zweckmäßigkeit umfasst.

1.2.2. Bundeseigene Verwaltung

Der Bund kann Bundesgesetze auch in bundeseigener Verwaltung ausführen:[24]

> *[1]Führt der Bund die Gesetze durch bundeseigene Verwaltung oder durch bundesunmittelbare Körperschaften oder Anstalten des öffentlichen Rechtes aus, so erläßt die Bundesregierung, soweit nicht das Gesetz Besonderes vorschreibt, die allgemeinen Verwaltungsvorschriften. [2]Sie regelt, soweit das Gesetz nichts anderes bestimmt, die Einrichtung der Behörden.*

Wann ein Fall der bundeseigenen Verwaltung vorliegt, ergibt sich aus Art. 86 GG jedoch nicht, sondern aus den Spezialvorschriften der Art. 87 ff. GG.[25]

Hervorzuheben ist insoweit Art. 87 Abs. 3 GG. Dieser eröffnet dem Bund auf Gebieten seiner Gesetzgebungskompetenz die Möglichkeit, ausnahmsweise Aufgaben durch Bundesgesetz an sich zu ziehen. Der Systematik des GG zufolge stellt die Gesetzgebungskompetenz des Bundes dabei allerdings die äußerste Grenze seiner Verwaltungskompetenzen dar.[26] Eine Zuständigkeit des Bundes für die Ausführung von Landesrecht ergibt sich danach – wie unter Punkt 1.2.1 bereits erwähnt – unter keinen Umständen.

Eine ausdrückliche Kompetenznorm des Bundes für den Vollzug von Bundesgesetzen im IT-Bereich findet sich in den Spezialvorschriften der Art. 87 ff. GG nicht. Für den Bereich des

[23] BVerfG, Beschluss vom 04.05.2010 – 2 BvL 8/07 u.a., NVwZ 2010, 1146 (1147 f.).
[24] Art. 86 GG; vgl. dazu Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 86, Rn. 1.
[25] Ebd.
[26] BVerfG, Urteil vom 30.10.1962 - 2 BvF 2/60, 1-3/61, NJW 1962, 2243 (2246).

bundeseigenen Vollzugs von Bundesrecht ist es dem Bund aber ohne weiteres möglich, seine eigene IT-Infrastruktur für ein digitalisiertes Verwaltungsverfahren zu regeln und bereitzustellen.[27] Denn für seine eigenen Behörden kann der Bundesgesetzgeber die Einrichtung der Behörden und das Verwaltungsverfahren – entweder als Annexkompetenz zur Sachmaterie oder in Ansehung des Art. 86 GG kraft Natur der Sache (vgl. dazu oben unter 1.1) – regeln.[28]

1.2.3. Selbstverwaltung der Kommunen

Aus staatsorganisationsrechtlicher Sicht sind die Kommunen Teil der Länder. Das GG konzipiert die Bundesrepublik Deutschland als zweistufigen Bundesstaat. Die Aufgaben und das Finanzgebaren der Kommunen werden daher grundsätzlich den Ländern zugerechnet.[29] Jedoch ergeben sich aus der grundgesetzlich besonders geschützten kommunalen Selbstverwaltung Besonderheiten, die sich auf den Vollzug von Bundes- und Landesgesetzen in den Kommunen und damit gegebenenfalls auch auf die Umsetzung einer zentralen Postfach- und Kommunikationslösung auswirken:

Art. 28 Abs. 2 GG garantiert die Selbstverwaltung von Gemeinden und Gemeindeverbänden. Diese Garantie geht über die Garantie der bloßen Existenz einer kommunalen Verwaltungsebene hinaus und gewährleistet in ihrer Ausprägung als sog. objektive

[27] Der Begriff der „Einrichtung" der Behörden in Art. 86 Satz 2 GG kann dabei unter anderem die Bereitstellung von IT-Basiskomponenten für den bundeseigenen Verwaltungsvollzug umfassen, siehe Schliesky: Verfassungsrechtliche Rahmenbedingungen des E-Government, DÖV 2004, S. 809 (811 f.), siehe auch Ibler, in: Dürig/Herzog/Scholz, Grundgesetz, Werkstand: 108. EL August 2025, Art. 86, Rn. 165.

[28] Schliesky: Verfassungsrechtliche Rahmenbedingungen des E-Government, DÖV 2004, S. 809 (813), siehe auch bereits BVerfG, Beschluss vom 15.07.1969 – 2 BvF 1/64, VerwRspr 1970, 142 (148), in dem das BVerfG betont, dass es keinem Zweifel unterliege, dass der Bund das Verfahren der bundeseigenen Verwaltung gesetzlich regeln könne, siehe auch Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 86, Rn. 9 und 13, der darauf hinweist, dass die Verbandskompetenz der Bundesebene in Art. 86 GG jedenfalls vorausgesetzt wird.

[29] BVerfG, Urteil vom 19.09.2018 – 2 BvF 1/15, 2 BvF 2/15, NVwZ 2018, 1703, Rn. 184.

Rechtsinstitutionsgarantie die eigenverantwortliche Aufgabenwahrnehmung durch die Kommunen.[30] Eine Zuweisung konkreter Aufgaben nimmt das GG dabei allerdings nicht vor.[31]

Im Einzelnen besagt Art. 28 Abs. 2 GG:

> *[1]Den Gemeinden muß das Recht gewährleistet sein, alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung zu regeln. [2]Auch die Gemeindeverbände haben im Rahmen ihres gesetzlichen Aufgabenbereiches nach Maßgabe der Gesetze das Recht der Selbstverwaltung. [3]Die Gewährleistung der Selbstverwaltung umfaßt auch die Grundlagen der finanziellen Eigenverantwortung; zu diesen Grundlagen gehört eine den Gemeinden mit Hebesatzrecht zustehende wirtschaftskraftbezogene Steuerquelle.*

Art. 28 Abs. 2 Satz 1 GG sichert den Gemeinden nach der Rechtsprechung des BVerfG einen grundsätzlich alle Angelegenheiten der örtlichen Gemeinschaft umfassenden Aufgabenbereich sowie die Befugnis zu eigenverantwortlicher Führung der Geschäfte in diesem Bereich zu.[32] Die Bestimmung schützt die Gemeinden dabei nicht nur vor einer ungerechtfertigten (unverhältnismäßigen) Entziehung ihrer Selbstverwaltungsaufgaben, sondern auch vor einer entsprechenden Zuweisung neuer, materiell staatlicher Aufgaben:[33]

Die Übertragung weiterer staatlicher Aufgaben birgt das Risiko einer Beeinträchtigung der kommunalen Selbstverwaltung, da die Wahrnehmung dieser Aufgaben zusätzliche finanzielle

---

30 Hellermann, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 28, Rn. 36 f.; siehe zur Ausprägung als institutionelle Rechtssubjektsgarantie und beschränkt-individuelle Rechtssubjektsgarantie auch BVerfG, Beschluss vom 12.05.1992 – 2 BvR 470/90, 2 BvR 650/90, 2 BvR 707/90, BeckRS 1992, 8123, Rn. 46.

31 Roth-Isigkeit, Verfassungsrechtliche Möglichkeiten der Aufgabenbündelung im Föderalstaat, Rechtsgutachten im Auftrag des Nationalen Normenkontrollrats (NKR), S. 20.

32 BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 30; unter „Angelegenheiten der örtlichen Gemeinschaft" versteht das BVerfG „diejenigen Bedürfnisse und Interessen, die in der örtlichen Gemeinschaft wurzeln oder auf sie einen spezifischen Bezug haben [...], die also den Gemeindeeinwohnern gerade als solchen gemeinsam sind, indem sie das Zusammenleben und -wohnen der Menschen in der (politischen) Gemeinde betreffen", siehe BVerfG, Beschluss vom 23.11.1988 – 2 BvR 1619/83, 2 BvR 1628/83, NVwZ 1989, 347 (350).

33 BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 30, 49 f. und 58.

und personelle Ressourcen bindet. Dies kann zur Folge haben, dass für die Erfüllung freiwilliger Selbstverwaltungsaufgaben nicht mehr ausreichend Ressourcen zur Verfügung stehen und der Handlungsspielraum der Kommunen entsprechend eingeschränkt wird.[34]

Art. 28 Abs. 2 GG garantiert den Kommunen zudem Eigenverantwortlichkeit bei der Art und Weise der Aufgabenerledigung und der Organisation ihrer Verwaltung.[35] Die Organisationshoheit ist nach Art. 28 Abs. 2 GG zwar lediglich im Rahmen der Gesetze gewährleistet und gilt damit grundsätzlich allein nach Maßgabe der gesetzlichen Ausgestaltung. Der Gesetzgeber muss den Kommunen allerdings nennenswerte organisatorische Befugnisse belassen und einen hinreichenden organisatorischen Spielraum bei der Wahrnehmung ihrer Aufgaben offenhalten. In jedem Fall muss gewährleistet sein, dass die Gemeinden bei ihrer inneren Organisation individuell auf die besonderen Anforderungen vor Ort durch eigene organisatorische Maßnahmen reagieren können. Die Organisationshoheit untersagt demnach staatliche Regelungen, die eine eigenständige organisatorische Gestaltungsfähigkeit ersticken würden. Ihr Kern darf nicht ausgehöhlt werden.[36]

Nach Art. 70 GG liegt die Gesetzgebungskompetenz für Gemeindeangelegenheiten grundsätzlich bei den Ländern. Der Bundesgesetzgeber darf in das kommunale Selbstverwaltungsrecht daher nur eingreifen, soweit das Grundgesetz selbst besondere Kompetenznormen vorsieht, die den Bund auch zu einer Einschränkung der gemeindlichen Selbstverwaltung ermächtigen. Das hat der verfassungsändernde Gesetzgeber durch den Erlass von Art. 84 Abs. 1 Satz 7 und Art. 85 Abs. 1 Satz 2 GG unterstrichen, die jeweils wortgleich lauten:[37]

> *Durch Bundesgesetz dürfen Gemeinden und Gemeindeverbänden Aufgaben nicht übertragen werden.*

Dieses Durchgriffsverbot steht in Zusammenhang mit der dem Bund eröffneten Möglichkeit, beim landeseigenen Vollzug von Bundesgesetzen abweichend vom Regelfall auch die

[34] BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 58.
[35] Ebd., Rn. 30 und 49.
[36] Ebd., Rn. 52 f.
[37] Ebd., Rn. 32.

Einrichtung der Behörden und das Verwaltungsverfahren zu regeln. Nach dem Durchgriffsverbot wird eine solche bundesrechtliche Regelung über die Einrichtung der Behörden, die den Kommunen die Erledigung einer Verwaltungsaufgabe aufgibt, ausgeschlossen.[38]

Das Durchgriffsverbot schützt die Organisationshoheit der Länder sowie die Finanzhoheit der Kommunen. Es soll insoweit vor allem verhindern, dass den Kommunen Aufgaben ohne Sicherstellung einer adäquaten Kostenerstattung übertragen werden.[39] Denn nach dem Konnexitätsgebot des Art. 104 a Abs. 1 GG würde die Finanzierungslast der Vollzugszuständigkeit folgen (dazu sogleich unter 1.3.1). Das GG sieht eine Erstattung bundesgesetzlich veranlasster Kosten bei den Kommunen im Grundsatz nicht vor.[40] Erfolgt die Aufgabenzuweisung hingegen durch den Landesgesetzgeber, greifen die landesverfassungsrechtlichen Konnexitätsregelungen,[41] die das Land – wenn auch in unterschiedlichem Umfang – zu einem Mehrbelastungsausgleich verpflichten.[42]

Eine Übertragung von Aufgaben im Sinne von Art. 84 Abs. 1 Satz 7 und Art. 85 Abs.1 Satz 2 GG läge immer dann vor, wenn den Kommunen mittels Bundesgesetzes erstmalig eine bestimmte (Verwaltungs-)Aufgabe zugewiesen oder eine damit funktional äquivalente Erweiterung einer bundesgesetzlich bereits zugewiesenen Aufgabe vorgenommen werden soll:[43] Eine erstmalige Aufgabenübertragung ist zu bejahen, wenn Kommunen durch Bundesgesetz eine bestimmte Tätigkeit zur Pflicht gemacht und ihnen insoweit die Sach- und / oder die Wahrnehmungskompetenz zugewiesen wird. Eine Erweiterung bereits bundesgesetzlich übertragener Aufgaben unterfällt dem Durchgriffsverbot dann, wenn sie in ihren Wirkungen auf das Schutzgut des Art. 28 Abs. 2 GG einer erstmaligen Aufgabenübertragung gleichkommt. Dies ist anzunehmen, wenn ihre Maßstäbe, Tatbestandsvoraussetzungen oder Standards so verändert werden, dass

38 BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 62.

39 Ebd., Rn. 33 und 66 f.; zu den von Art. 28 Abs. 2 GG geschützten Gewährleistungsinhalten zählt ausdrücklich auch die kommunale Finanzhoheit (Satz 3), die das Recht zu eigenverantwortlicher Einnahmen- und Ausgabenwirtschaft beinhaltet, siehe BVerfG, Beschluss vom 27.01.2010 – 2185/04 u.a., NVwZ 2010, 895 (898).

40 BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 71.

41 Ebd., Rn. 67.

42 Ebd., Rn. 69.

43 Ebd., Rn. 48 und 83.

damit mehr als unerhebliche Auswirkungen auf die Organisations-, Personal- und Finanzhoheit der Kommunen verbunden sind, etwa wenn das Änderungsgesetz den Kommunen neue Organisationspflichten auferlegt. Für das regulatorische Interesse des Bundes ist dagegen nur Raum, wenn die Auswirkungen auf die Eigenverantwortlichkeit der Kommunen gering sind.[44]

1.2.4. Zusammenfassung: Vollzugszuständigkeiten und diesbezügliche Regelungsbefugnisse als Ausgangslage

Im Grundsatz ergibt sich ausgehend von den Art. 83 ff. GG damit folgendes Bild:

	Vollzugskompetenzen	Regelungs- und Organisationskompetenz
Bund	Vollzug von Bundesrecht durch bundeseigene Verwaltung (Art. 86 GG)	Ungeschriebene Bundeskompetenz für Organisations- und Verfahrensrecht (Natur der Sache oder Annexkompetenz zur Sachmaterie)
Länder	Vollzug von Landesrecht	Regelung von Einrichtung der Behörden (u.a. Aufgabenzuweisung und sachliche Ausstattung) und Verwaltungsverfahren durch Länder
	Vollzug von Bundesrecht als eigene Angelegenheit (Art. 83 GG)	Grds. Regelung von Einrichtung der Behörden und Verwaltungsverfahren durch Länder; Bund kann Regelungen treffen, von denen die Länder allerdings nur in Ausnahmefällen (bzgl. Verwaltungsverfahren) nicht abweichen dürfen
	Vollzug von Bundesrecht als Bundesauftragsverwaltung (Art. 85 GG)	Grds. Regelung von Einrichtung der Behörden durch Länder; Bund darf Verwaltungsverfahren sowie mit Zustimmung des Bundesrates auch Behördeneinrichtung regeln; weitere Einwirkung über VV, Weisungen, Aufsicht.
Gemeinden	Vollzug von Bundes- und Landesrecht	Grds. Durchgriffsverbot für Bund - Länder regeln Organisation und Verfahren; Art. 28 Abs. 2 GG zu beachten: Organisationshoheit und -freiheit der Gemeinde im Rahmen der Gesetze sowie Schutz gegen übermäßige Vorgaben/Aufgabenübertragung

Abbildung 1: Vollzugszuständigkeiten und Regelungsbefugnisse – Überblick

Die in der Tabelle benannten Regelungs- und Organisationskompetenzen erstrecken sich grundsätzlich auch auf die Bereitstellung und Vorgaben zur Verwendung bestimmter IT-Infrastrukturen. Jedoch werden Regelungen in diesem Bereich zum Teil durch die besonderen Kompetenzen des Art. 91c GG überlagert. Die konkreten Auswirkungen dieser grundsätzlichen Kompetenzordnung auf die Machbarkeit und Ausgestaltung von ZaPuK ergeben sich daher erst unter Berücksichtigung der Besonderheiten des Art. 91c GG (dazu sogleich unter 1.4) und werden auf dieser Grundlage konkret in Abschnitt 2 untersucht.

[44] BVerfG, Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 84 bis 86.

1.3. Ausgangspunkt III: Bei der Regelung und Ausübung der Verwaltungskompetenzen zu beachtende Grundsätze

Als fundamentale in der Verfassung zum Ausdruck kommende Grundsätze sind im Rahmen der Ausübung und Umsetzung von Verwaltungsaufgaben der Konnexitätsgrundsatz (Punkt 1.3.1), der Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung (Punkt 1.3.2) sowie das Verbot der Mischverwaltung (Punkt 1.3.3) zu beachten.

1.3.1. Konnexitätsgrundsatz – Zusammenspiel zwischen Aufgabenordnung und Finanzierung

Bund und Länder können bei der Finanzierung von Verwaltungsaufgaben nicht frei agieren, sondern haben die in Abschnitt X des GG festgelegten Zusammenhänge zwischen verfassungsrechtlicher Aufgabenzuordnung und Finanzierungslast zu beachten. Daher muss bei der rechtlichen Ausgestaltung von ZaPuK und bei der Wahl einer passenden Rechtsgrundlage stets mitgedacht werden, wie sich dies auf die entsprechenden Finanzierungspflichten bzw. Möglichkeiten zur Gestaltung der Finanzierung auswirkt.

Nach der in Art. 104a Abs. 1 GG niedergelegten allgemeinen Lastenverteilungsregel tragen – beim Fehlen anderweitiger verfassungsrechtlicher Regelungen – Bund und Länder jeweils die sich aus der Wahrnehmung ihrer jeweiligen Aufgaben ergebenen Ausgaben (sog. *Konnexitätsgrundsatz*).[45]

Art. 104a Abs. 1 GG bestimmt insofern ausdrücklich:

> *Der Bund und die Länder tragen gesondert die Ausgaben, die sich aus der Wahrnehmung ihrer Aufgaben ergeben, soweit dieses Grundgesetz nichts anderes bestimmt.*[46]

[45] Heun, in: Dreier, Grundgesetz, Kommentar, 3. Auflage 2018, Art. 104a, Rn. 12; Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 63. Edition, Stand: 15.09.2025, Art. 104a, Rn. 5.

[46] Die Vorschrift gilt für das Verhältnis zwischen Bund und Ländern. Im Verhältnis zwischen dem Bund und den Kommunen entfaltet Art. 104a Abs. 1 GG dagegen keine unmittelbare Wirkung. Die Wirkung ergibt sich jedoch mittelbar daraus, dass die Kommunen aus staatsorganisationsrechtlicher und finanzverfassungsrechtlicher Sicht den Ländern zugeordnet werden, siehe Kube, in: BeckOK

Die bundesstaatliche Finanzverfassung folgt damit den allgemeinen Kompetenzregeln des GG und knüpft an die sich daraus ergebenden Aufgabenzuweisungen an.[47] Unter der *Aufgabenwahrnehmung* ist der Aufgabenvollzug, also die Ausübung der Verwaltungskompetenzen zu verstehen. Die Finanzierungszuständigkeit ist somit an die Verwaltungszuständigkeit der jeweiligen Hoheitsträger gekoppelt.[48]

Die Finanzverfassung des GG begründet nach der Rechtsprechung des BVerfG eine in sich geschlossene Rahmen- und Verfahrensordnung, die den einfachen Gesetzgeber an den durch sie gesetzten Rahmen bindet. Analogieschlüssen ist der Boden entzogen. Weder der Bund noch die Länder können über ihre im GG festgelegten Finanzierungskompetenzen verfügen. Eine Kompetenzverschiebung hält das BVerfG insofern auch mit Zustimmung der Beteiligten für unzulässig.[49] Aus der Finanzierungskompetenz ergibt sich nicht nur eine Finanzierungsbefugnis, sondern auch eine Finanzierungspflicht. Art. 104a Abs. 1 GG schützt die Gebietskörperschaften vor finanziellen Belastungen, die nicht aus ihrem eigenen Aufgabenbereich erwachsen. Die Vorschrift schließt darüber hinaus eine Mischfinanzierung aus und untersagt Formen freiwilliger Fremdfinanzierung, durch die Einfluss auf die Aufgabenwahrnehmung der jeweils anderen Ebene genommen werden könnte („goldener Zügel"). Der Bund ist insofern daran gehindert, freiwillig Länderaufgaben zu finanzieren.[50]

Außerhalb der im Grundgesetz niedergelegten Ausnahmen sind keine Abweichungen vom Konnexitätsgrundsatz zulässig. Solche Ausnahmen finden sich aber in den Absätzen 2-4 des Art. 104a GG – gemäß Art. 104a Abs. 2 GG trägt etwa der Bund die sich aus der

Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 104a, Rn. 8; BVerfG, Urteil vom 27.05 1992 – 2 BvF 1/88, BeckRS 1992, 118483; BVerwG, Urteil vom 08.02.1974 – VII C 16/71, NJW 1974, 1207 (1210 f.); Urteil vom 30.11.1995 – 7 C 56/93, NVwZ 1996, 595 (596).

47 Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 104a, Rn. 2; Schwarz, in: Dürig/Herzog/Scholz Grundgesetz, Lfg. 103 Januar 2024, Art. 104a, Rn. 3.

48 BVerfG, Beschluss vom 15.11.2023 – 2 BvG 1/19, 2 BvG 1/21, NVwZ 2024, 50 (51), Rn. 54; BVerfG, Beschluss vom 15.07.1969 – 2 BvF 1/64, VerwRspr 1970, 142 (160); Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 104a, Rn. 9; Siekmann, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 104a, Rn. 4, m.w.N.

49 BVerfG, Urteil vom 28.03.2002 – 2 BvG 1/01 u.a., NJW 2002, 2020

50 Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 104a, Rn. 5.

Bundesauftragsverwaltung ergebenden Ausgaben der Länder –[51] und in den Gemeinschaftsaufgaben nach Art. 91a, 91b, 91c und 91e GG.[52]

Eine Sonderregel sieht jedoch wiederum Art. 104a Abs. 5 Satz 1 Halbsatz 1 GG vor: Danach verbleiben „Verwaltungsausgaben" stets bei der handelnden Körperschaft.[53] Sie sind ausnahmslos von der jeweiligen Ebene – Bund oder Länder - zu tragen, bei deren Behörden sie anfallen. „Verwaltungsausgaben" in diesem Sinne sind die Ausgaben für die Unterhaltung und den Betrieb des Verwaltungsapparats – also für das Verwaltungspersonal und die Verwaltungseinrichtungen. Sie lassen sich anschaulich mit Gemeinkosten vergleichen, da sie einer konkreten Verwaltungsleistung nur indirekt zugeordnet werden können.[54] Für die von der Grundnorm des Art. 104a Abs. 1 GG ebenfalls erfassten „Zweckausgaben" gilt diese Vorgabe nicht, sie können demnach durch im GG vorgesehene Ausnahmeregelungen von einer anderen föderalen Ebene übernommen werden. „Zweckausgaben" sind solche, die unmittelbar im Zusammenhang mit der Verwirklichung des Verwaltungszwecks stehen, d.h. unmittelbar der Umsetzung der jeweiligen Verwaltungsaufgabe dienen.[55] Einschränkend kann sich diese Differenzierung insbesondere auf die Finanzierungsverantwortung des Bundes im Fall der Auftragsverwaltung sowie bei der Finanzierung der Ausführung von Bundes- oder Landesrecht durch die Kommunen auswirken, da in diesen Fällen die Verwaltungsausgaben weiter von der ausführenden Körperschaft zu tragen sind.[56] Die Abgrenzung zu den Zweckausgaben wird dabei allerdings nicht immer eindeutig sein:

Auch bei der Umsetzung von IT-Infrastrukturprojekten auf Grundlage der Sondervorschriften in Art. 91c GG (dazu sogleich unter 1.4) ist grundsätzlich möglich, dass Art. 104a Abs. 5 Satz 1 Halbsatz 1 GG auf Finanzierungsregelungen Anwendung findet, soweit in diesen vom Konnexitätsgrundsatz abgewichen werden soll und auf Grundlage von Art. 91c GG gegebenenfalls auch abgewichen werden darf. Jedoch ist in solchen Fällen regelmäßig die Einrichtung der

[51] Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 104a, Rn. 28 f., der jedoch betont, dass dies nur für die Zweckausgaben gelte.
[52] Siekmann, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 104a, Rn. 2.
[53] Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 65. Edition, Stand: 01.03.2026, Art. 104a, Rn. 46.
[54] Ebd., Rn. 22.
[55] Ebd., Rn. 23; Siekmann, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 104a, Rn. 9.
[56] Siekmann, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 104a, Rn. 9.

Verwaltungsbehörden im Sinne einer Ausstattung mit IT-Infrastruktur der Hauptzweck des jeweiligen Vorhabens und der zugrundeliegenden Rechtsgrundlage, eine Differenzierung zwischen allgemeinen Verwaltungsausgaben und den unmittelbar mit dem Verwaltungszweck verbundenen Zweckausgaben erscheint daher kaum möglich, sodass viel dafür spricht, dass sich Art. 104a Abs. 5 Satz 1 Halbsatz 1 GG in diesen Fällen nicht auswirkt.

Folgerungen für die Governance von ZaPuK

Im Ergebnis bleibt festzuhalten, dass der Konnexitätsgrundsatz gemäß Art. 104a Abs. 1 GG als zentrale Finanzierungsregel der föderalen Verfassung des Grundgesetzes bei der Ausgestaltung von ZaPuK maßgeblich zu berücksichtigen ist und insbesondere bei der Prüfung und Auswahl möglicher verfassungsrechtlicher Grundlagen für das Vorhaben mitgedacht werden muss. Im Wesentlichen folgen aus dem Konnexitätsgrundsatz die folgenden Vorgaben:

- Die Finanzierungszuständigkeit folgt der Verwaltungszuständigkeit.
- Ausnahmen hiervon müssen im Grundgesetz verankert sein.
- Auch Formen der freiwilligen Fremdfinanzierung oder Mischfinanzierung sind ohne eine solche verfassungsrechtliche Grundlage unzulässig.

1.3.2. Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung

Weiter ist im Zusammenhang mit der rechtlichen Ausgestaltung von ZaPuK der „Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung“ bei der Ausführung von Verwaltungsaufgaben zu beachten. Danach haben Verwaltungsträger die ihnen zugewiesene Verwaltungsaufgabe grundsätzlich durch ihre eigenen Verwaltungseinrichtungen – mit eigenen personellen und sachlichen Mitteln – wahrzunehmen. Abweichungen davon durch Inanspruchnahme von „Hilfe“ kompetenzfremder Verwaltungsträger sind nur in sehr engen Grenzen möglich und würden insbesondere nur hinsichtlich einer eng umgrenzten Verwaltungsmaterie in Betracht kommen.[57]

[57] BVerfG, Beschluss vom 12.01.1983 – 2 BvL 23/81, NVwZ 1983, 537 (541).

1.3.3. Verbot der Mischverwaltung

Schließlich ist bei der Ausgestaltung und Governance von ZaPuK auch das sog. Verbot der Mischverwaltung zu berücksichtigen. Das GG untersagt eine solche Mischverwaltung, soweit sie nicht ausdrücklich zugelassen ist.[58] Wie bereits dargestellt, trifft das GG eine klare und erschöpfende Zuordnung der Verwaltungszuständigkeiten. Kompetenzverlagerungen zwischen Bund und Ländern sind ebenso wie die Zusammenführung von Verwaltungseinrichtungen aus Bundes- und Länderebene ohne entsprechende verfassungsrechtliche Grundlage daher selbst mit Zustimmung der Beteiligten unzulässig.[59] Insbesondere genügt es auch nicht, für Zwecke der Verwaltungsdigitalisierung darauf zu verweisen, dass diese naturgemäß eine ebenenübergreifende Zusammenarbeit erfordere; vielmehr muss auch insoweit eine Abweichung vom Verbot der Mischverwaltung zwischen Bund und Ländern ausdrücklich verfassungsrechtlich erlaubt sein.[60]

Eine der Regelungen, die ausnahmsweise eine solche gemeinschaftliche Zusammenarbeit erlauben, stellt Art. 91c GG dar:

1.4. Sondervorschrift für die Zusammenarbeit im IT-Bereich: Art. 91c GG

In Abschnitt VIIIa enthält das GG unter der Überschrift „Gemeinschaftsaufgaben, Verwaltungszusammenarbeit" in den Art. 91a–e GG Bestimmungen, die dem Bund und den Ländern die Möglichkeit für ein kooperatives Zusammenwirken eröffnen.[61]

Art. 91c GG bildet dabei die Grundlage für die Zusammenarbeit von Bund und Ländern auf dem Gebiet der Informationstechnik [62] und beinhaltet insoweit eine konstitutive verfassungsrechtliche Erlaubnis zur Abweichung von dem Verbot der Mischverwaltung[63]. Die Norm schafft damit die verfassungsrechtliche Basis für ein tatsächliches sowie rechtliches Zusammenwirken

[58] BVerfG, Urteil vom 20.12.2007 – 2 BvR 2433/04 u.a., NVwZ 2008, 183 (186), Rn. 153; BVerfG, Urteil vom 15.07.2003 – 2 BvF 6/98, MMR 2003, 664 (666).
[59] BVerfG, Urteil vom 15.07.2003 – 2 BvF 6/98, MMR 2003, 664 (666).
[60] Vgl. Siekmann/Thiel, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 91c, Rn. 4 f.
[61] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 64. Edition, Stand: 15.09.2025, Art. 91a.
[62] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 3.
[63] Siekmann/Thiel, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 91c, Rn. 4 f.

der Gebietskörperschaften innerhalb des IT-Bereichs,[64] das angesichts der ansonsten grundsätzlich getrennten und in Art. 83 ff. GG abschließend geregelten Verwaltungszuständigkeiten einer ausdrücklichen verfassungsrechtlichen Ermächtigung bedarf[65].

Unter dem Begriff der informationstechnischen Systeme versteht die Gesetzesbegründung zu Art. 91c GG dabei die „technischen Mittel zur Verarbeitung und Übertragung von Informationen".[66]

Nach der in Art. 91c Abs. 1 GG verankerten Generalklausel können Bund und Länder hinsichtlich der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken. Die eröffneten Handlungsspielräume werden in Art. 91c Abs. 2 und 3 GG näher konkretisiert: Bund und Länder können die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen auf Grund von Vereinbarungen festlegen (Abs. 2 Satz 1); die Länder darüber hinaus auch – ohne den Bund – den gemeinschaftlichen Betrieb informationstechnischer Systeme und die Errichtung von dazu bestimmten Einrichtungen vereinbaren (Abs. 3). Demgegenüber wird in Art. 91c Abs. 4 und 5 GG eine herausgehobene Kompetenzstellung des Bundes begründet: Während Art. 91c Abs. 4 GG dem Bund die Befugnis verleiht, ein Verbindungsnetz zur Verbindung der informationstechnischen Netze des Bundes und der Länder zu errichten, greift Art. 91c Abs. 5 GG tiefer in das föderale Kompetenzgefüge ein und ermächtigt den Bund zur Regelung eines übergreifenden informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern.[67]

Inwieweit diese verschiedenen Rechtsgrundlagen für die Errichtung und den Betrieb von ZaPuK herangezogen werden können, wird im Einzelnen in Abschnitt 2.2 untersucht.

---

[64] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 3.
[65] Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 6.
[66] Begründung zu Art. 91c GG, Gesetzentwurf der Fraktionen der CDU/CSU und SPD, BT-Drucksache 16/12410 vom 24.03.2009, S. 8.
[67] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 12 f.

1.5. Sondervorschrift für den Bereich der Finanzverwaltung: Art. 108 GG

Weitere für ZaPuK relevante Sonderregelungen enthält Abschnitt X des Grundgesetzes. Art. 108 GG normiert für den Bereich der Finanzverwaltung als lex specialis zu den Art. 83 ff. GG die verfassungsrechtliche Verteilung der Steuerverwaltungshoheit[68] zwischen Bund und Ländern.[69]

Hierbei wird zwischen der Bundesverwaltung (Abs. 1), der Landeseigenverwaltung (Abs. 2) und der Landesverwaltung im Auftrag des Bundes (Abs. 3) unterschieden:[70] In dem in Art. 108 Abs. 1 Satz 1 GG enthaltenen Katalog werden die einzelnen Steuern aufgelistet, die durch die Bundesfinanzbehörden verwaltet werden. Art. 108 Abs. 2 Satz 1 GG ordnet die Verwaltungskompetenz für die übrigen Steuern den Landesfinanzbehörden zu. Verwalten die Landesfinanzbehörden Steuern, die ganz oder zum Teil dem Bund zufließen, werden sie im Auftrag des Bundes tätig (Art. 108 Abs. 3 Satz 1 GG).

Ferner enthält Art. 108 GG spezielle Gesetzgebungskompetenzen des Bundes zum Finanzorganisationsrecht und zum Finanzverfahrensrecht:[71]

Der Aufbau der Bundesfinanzbehörden wird gemäß Art. 108 Abs. 1 Satz 2 GG durch Bundesgesetz geregelt. Der Bund kann mit Zustimmung des Bundesrates daneben gesetzlich auch den Aufbau der Landesfinanzbehörden und die einheitliche Ausbildung der Beamten regeln (Art. 108 Abs. 2 Satz 2 GG). Der Begriff „Aufbau" weicht dabei von der Terminologie der allgemeinen Vorschriften ab, wird aber wohl überwiegend mit dem in Art. 84 Abs. 1 Satz 1, 85 Abs. 1 Satz 1, 86 Satz 2 GG verwendeten Begriff „Einrichtung" gleichgesetzt, der sowohl die Errichtung einer neuen als auch die nähere Ausgestaltung einer bereits vorhandenen Behörde umfasst, einschließlich der organisatorisch-personellen Ausstattung sowie der Kompetenzen. Diese Regelungen sind nicht nur auf die Ausführung von Bundesgesetzen beschränkt, sondern gelten auch für den Vollzug von Landesgesetzen, bezüglich dessen der Bund nach den

[68] Die in Art. 108 GG geregelten Verwaltungskompetenzen betreffen die Verwaltung aller Steuern und Abgaben, auf die sich Art. 105 und 106 GG beziehen, siehe Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 64. Edition, Stand: 15.11.2025, Art. 108, Rn. 1.

[69] BVerfG, Beschluss vom 27.06.2002 – 2 BvF 4/98, NVwZ 2003, 595 (597).

[70] Siekmann/Drüen, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 108, Rn. 6.

[71] Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 64. Edition, Stand: 15.11.2025, Art. 108, Rn. 1.

allgemeinen Vorschriften hingegen keine Einwirkungsmöglichkeiten besitzt.[72] Von seiner Gesetzgebungskompetenz hat der Bund durch Regelungen im Finanzverwaltungsgesetz (FVG) Gebrauch gemacht.[73]

Art. 108 Abs. 5 Satz 1 GG normiert ferner eine ausschließliche Gesetzgebungskompetenz des Bundes für das von den Bundesfinanzbehörden anzuwendende Verfahren. Entsprechende einfachgesetzliche Regelungen finden sich insbesondere in der Abgabenordnung (AO). Der Bund kann darüber hinaus gemäß Art. 108 Abs 5. Satz 2 GG auch das von den Landesfinanzbehörden anzuwendende Verfahren durch zustimmungsbedürftiges Bundesgesetz regeln – unabhängig davon, ob der Bund die materiell-rechtliche Gesetzgebungskompetenz für die betreffende Steuer besitzt.[74]

Art. 108 Abs. 4 Satz 1 GG eröffnet dem Bundesgesetzgeber zudem die Möglichkeit, zur Verbesserung oder Erleichterung des Steuervollzugs ein Zusammenwirken von Bundes- und Landesfinanzbehörden im Sinne einer Mischverwaltung vorzusehen oder die Verwaltung einzelner Steuern abweichend von Art. 108 Abs. 1 und 2 GG zuzuordnen. Auch insoweit besteht eine ausschließliche Gesetzgebungskompetenz des Bundes.[75]

Auch wenn sich dies aus dem Wortlaut der Vorschrift nicht unmittelbar ergibt, ist die in Art. 108 Abs. 4 GG niedergelegte Möglichkeit der bund- und länderübergreifenden Kooperation insbesondere für eine ebenübergreifende Zusammenarbeit im IT-Bereich relevant.

Auf Basis von Art. 108 Abs. 4 Satz 3 GG können dabei auch verbindliche Mehrheitsentscheidungen für alle Länder getroffen werden.[76] Die Regelung wurde mit der Verfassungsänderung im Jahr 2017 in das GG aufgenommen. In ihrer ursprünglichen Konzeption sollte sie sich

[72] Siekmann/Drüen, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 108, Rn. 18 und 21 f.
[73] Schenke, in: Grundgesetz für jede(n), Der Grundgesetzkommentar von Prof. Dr. Helge Sodan, Art. 108 Rn. 5, abrufbar unter https://www.grundgesetz-fuer-jeden.de/artikel-108.html), zuletzt abgerufen am 20.01.2026.
[74] Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 64. Edition, Stand: 15.11.2025, Art. 108, Rn. 7 und 11.
[75] Ebd., Art. 108, Einleitung und Rn. 4, nach dem auch die Kostenersparnis die Voraussetzung der Verbesserung oder Erleichterung des Steuervollzugs erfüllt.
[76] Siekmann/Drüen, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 108, Rn. 36.

sachlich ausdrücklich auf den Bereich der Informationstechnik beschränken[77] und laut Gesetzesbegründung klarstellen, dass die Gesetzgebungskompetenz des Bundes bezüglich des Zusammenwirkens in diesem Bereich sowohl bei der Entwicklung als auch beim Einsatz von automatischen Einrichtungen in der Steuerverwaltung die Möglichkeit umfasst, alle Länder bindende Mehrheitsentscheidungen vorzusehen.[78] Eine Beschränkung auf den IT-Bereich ist im Laufe des Gesetzgebungsverfahrens entfallen und findet sich in der nun geltenden Fassung des Art. 108 Abs. 4 Satz 3 GG nicht mehr wieder.[79]

Obwohl der Anwendungsbereich im Gesetzgebungsverfahren auf alle Bereiche der Zusammenarbeit von Bund und Ländern bei der Steuerverwaltung ausgeweitet wurde, kommt der Bestimmung insbesondere im Hinblick auf die Entwicklung und den Einsatz von IT in der Steuerverwaltung besondere Bedeutung zu.[80]

2. Untersuchung potenzieller verfassungsrechtlicher Rechtsgrundlagen für das Vorhaben

Im Folgenden soll untersucht werden, welche verfassungsrechtlichen Rechtsgrundlagen für die Realisierung einer einheitlichen föderalen Postfach- und Kommunikationsinfrastruktur in Betracht kommen und inwieweit deren Reichweite und Vorgaben jeweils die nach dem derzeitigen Stand der Zielarchitektur für Postfach- und Kommunikationslösungen angestrebte Ausgestaltung und Governance abbilden können.

Wie bereits aufgezeigt, besteht für den Bund im Hinblick auf die **Ausführung von Bundesrecht** die Möglichkeit, Einfluss auf das Verwaltungsverfahren der Länder zu nehmen. Daher soll

---

[77] Der Gesetzesentwurf sah ursprünglich die folgende Formulierung für Art. 108 Abs. 4 Satz 3 GG vor: *Das Bundesgesetz nach Satz 1 kann im Bereich der Informationstechnik für ein Zusammenwirken von Bund und Ländern bestimmen, dass bei Zustimmung einer im Gesetz genannten Mehrheit Regelungen für den Vollzug von Steuergesetzen für alle Länder verbindlich werden*, siehe Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 8.

[78] Begründung zu Art. 108 Abs. 4 Satz 3 GG, Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 18 f.

[79] Kube, in: BeckOK Grundgesetz, Epping/Hillgruber, 64. Edition, Stand: 15.11.2025, Art. 108, Rn. 4; Siekmann/Drüen, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 108, Rn. 35.

[80] Schenke, in: Grundgesetz für jede(n), Der Grundgesetzkommentar von Prof. Dr. Helge Sodan, Art. 108 Rn. 13, abrufbar unter https://www.grundgesetz-fuer-jeden.de/artikel-108.html), zuletzt abgerufen am 20.01.2026.

nachfolgend zunächst dargestellt werden, welche Bedeutung dies für die Realisierung der Postfach- und Kommunikationsstruktur haben könnte (Punkt 2.1). Dabei ist jedoch zu beachten, dass sich die Betrachtung ausschließlich auf die Ausführung von Bundesrecht beschränkt.

Für eine Ausgestaltung der Postfach- und Kommunikationsstruktur, die auch die **Ausführung von Landesrecht** sowie nach Möglichkeit auch eine Bindungswirkung gegenüber den **Kommunen** mitberücksichtigt, kommt Art. 91c GG mit den dort enthaltenen Ausnahmen vom Verbot der Mischverwaltung als zentrale verfassungsrechtliche Grundlage in Betracht (dazu Abschnitt 2.2).

2.1. Regelungs- und Organisationskompetenz des Bundes bei der Ausführung von Bundesgesetzen (Art. 84-86 GG)

2.1.1. Bundeseigene Verwaltung

Für den Bereich der Bundesgesetzgebung, dessen Vollzug durch die bundeseigene Verwaltung – also gemäß Art. 86 ff. GG durch Verwaltungseinrichtungen des Bundes – erfolgt, ist die Bereitstellung einer Postfach- und Kommunikationsinfrastruktur aus kompetenzrechtlicher Sicht weitgehend unproblematisch. Im bundeseigenen Vollzug kann der Bund seine IT-Infrastruktur für ein digitalisiertes Verwaltungsverfahren selbst gestalten, bereitstellen und betreiben (siehe hierzu bereits 1.2.2). Ihm obliegt dabei auch gemäß Art. 104a Abs. 1 GG die Finanzierung.

2.1.2. Ausführung von Bundesrecht durch die Länder als eigene Angelegenheit

Im Bereich der Ausführung von Bundesrecht durch die Länder als eigene Angelegenheit erscheint eine verbindliche Regelung der Anbindung der Länder an die Postfach- und Kommunikationsinfrastruktur des Bundes möglich. In Betracht kommt insoweit, dass der Bund in Bezug auf die Vorgabe einer Postfach- und Kommunikationsinfrastruktur im Bereich des Bundesrechts, das von den Ländern gemäß Art. 83 GG als eigene Angelegenheit ausgeführt wird, von seiner auf die Einrichtung der Behörden und das Verfahrensrecht bezogenen Gesetzgebungskompetenz Gebrauch und den Ländern punktuell Vorgaben für die Nutzung der IT-Infrastruktur macht (siehe zuvor unter 1.2.1.a)). Dabei kann dahinstehen, ob sich diese Kompetenz als ungeschriebene Annexkompetenz zur Regelung der Sachmaterie der in den Art. 70 ff. GG

niedergelegten Regelungsbefugnisse ableitet oder direkt durch Art. 84 Abs. 1 Satz 2 Halbsatz 1 GG begründet wird. Für eine effektive Umsetzung ist jedoch eine grundsätzliche Kooperationsbereitschaft der Länder erforderlich. Denn diesen steht es gemäß Art. 84 Abs. 1 Satz 2 Halbsatz 2 GG frei, von den Vorgaben des Bundes durch eigene Regelungen abzuweichen. Selbst für den Fall, dass der Bund gemäß Art. 84 Abs. 1 Satz 5 GG das Verwaltungsverfahren im Ausnahmefall wegen eines besonderen Bedürfnisses nach bundeseinheitlicher Regelung ohne Abweichungsmöglichkeit für die Länder regelt, bedarf er dafür gemäß Art. 84 Abs. 1 Satz 6 GG der Zustimmung des Bundesrates.

Die Ausgaben, die sich im Zusammenhang mit dem Anschluss an und der Nutzung von ZaPuK ergeben, wären im Rahmen der Reichweite von Art. 84 GG nach den allgemeinen Grundsätzen des Art. 104a GG von den Ländern zu tragen.

2.1.3. Bundesauftragsverwaltung durch die Länder

Auch für den Vollzug solcher Gesetze, die Gegenstand der Bundesauftragsverwaltung sind, ist eine solche – ggf. sogar als Anschlusspflicht an eine Postfach- und Kommunikationsinfrastruktur des Bundes ausgestaltete – Regelung durch ein Bundesgesetz denkbar. Denn im Kontext der Bundesauftragsverwaltung hat der Bund – wie zuvor unter 1.2.1.b) dargestellt – gemäß Art. 85 Abs. 1 Satz 1 GG nicht nur die Befugnis, die Einrichtung der Behörden („soweit nicht Bundesgesetze mit Zustimmung des Bundesrates etwas anderes bestimmen"), sondern auch das Verwaltungsverfahren gesetzlich zu regeln. Regelungen, die die Einrichtung der Behörde betreffen, erfordern jedoch die Zustimmung des Bundesrates.

Beschränkt sind auch in dieser Variante die Gestaltungsmöglichkeiten hinsichtlich der Finanzierungsverantwortung für die entsprechende Infrastruktur. Nach dem **Konnexitätsgrundsatz** tragen grundsätzlich die für den Verwaltungsvollzug zuständigen Länder die damit verbundenen Ausgaben. Im Rahmen der Bundesauftragsverwaltung übernimmt zwar der Bund gemäß Art. 104a Abs. 2 GG die betreffenden Zweckausgaben, dies gilt aber gemäß Art. 104a Abs. 5 Satz 1 Halbsatz 1 GG wiederum grundsätzlich nicht für die allgemeinen Verwaltungsausgaben – unter die regelmäßig auch die allgemeinen Kosten für den Anschluss an eine vom Bund bereitgestellte Infrastruktur fallen dürften. Komplexität und Mehraufwand ergäben sich in dieser

Konstellation daraus, dass die darüber hinausgehenden, an bestimmte Sachaufgaben geknüpften Mehraufwände (Zweckausgaben) jeweils anhand ihrer Zuordnung zu Aufgaben des Bundes oder der Länder konkret aufgeschlüsselt und verteilt werden müssten, um der Gefahr einer Mischfinanzierung zu begegnen (vgl. zum Ganzen bereits Abschnitt 1.3.1).

Die Regelungsbefugnis des Bundes wird schließlich **in beiden Varianten** des Verwaltungsvollzugs durch die Länder – landeseigene und Bundesauftragsverwaltung – durch das kommunale **Durchgriffsverbot** in seiner Reichweite begrenzt (vgl. bereits unter 1.2.3). Für die kommunale Ebene kann ein Bundesgesetz daher eine Postfach- und Kommunikationsinfrastruktur nur insoweit vorgeben, als damit kein erheblicher Aufwand für die Kommunen verbunden ist, der funktional einer unzulässigen Aufgabenübertragung vergleichbar wäre (vgl. hierzu auch die Ausführungen in Abschnitt 2.2.2.a)cc)).

2.1.4. Folgerungen für die Machbarkeit von ZaPuK

Als Rechtsgrundlagen für die Realisierung von ZaPuK kommen die vorstehenden Regelungskompetenzen nur sehr eingeschränkt in Betracht:

- Ohne die Einbeziehung weiterer verfassungsrechtlicher Rechtsgrundlagen kann die Umsetzung von ZaPuK bereits deshalb nicht von den Art. 84 ff. GG getragen werden, weil deren Reichweite auf die Ausführung von Bundesgesetzen begrenzt ist.

- Eine Regelung auf Grundlage von Art. 86 GG wäre in ihrer Reichweite zudem noch enger begrenzt, auf den Vollzug von Bundesgesetzen in bundeseigenen Behörden. Jedoch bietet Art. 86 GG den Vorteil, dass der Bund auf dieser Basis ZaPuK – wenn auch zunächst nur für einen begrenzten Anwendungsbereich – zentral entwickeln, bereitstellen, betreiben und finanzieren könnte (siehe dazu noch näher unter 2.3).

- Auf Grundlage von Art. 84 GG und Art. 85 GG könnte der Bund zwar grundsätzlich im Rahmen von Verwaltungsverfahren und Behördeneinrichtung auch den Anschluss an eine einheitliche Postfach- und Kommunikationsinfrastruktur regeln. Nicht abgedeckt wäre jedoch weiterhin die Ausführung von Landesrecht. Darüber hinaus wäre auch in diesem begrenzten Rahmen eine umfassende Finanzierung von ZaPuK durch den

Bund nicht abbildbar. Im Rahmen der Ausführung durch die Länder als eigene Angelegenheit läge dort auch die Finanzierungsverantwortung; im Zusammenhang mit der Bundesauftragsverwaltung wäre eine kleinteilige Aufschlüsselung der Finanzierungsanteile von Bund und Ländern erforderlich.

2.2. Zusammenarbeit von Bund und Ländern im IT-Bereich (Art. 91c GG)

Im Folgenden soll geprüft werden, ob Art. 91c GG eine geeignete Rechtsgrundlage für das gegenständliche IT-Infrastrukturvorhaben enthält, die über die Ausführung von Bundesrecht hinaus auch die **Ausführung von Landesrecht** berücksichtigt.

2.2.1. Bundeskompetenz nach Art. 91c Abs. 4 GG – Errichtung und Betrieb eines Verbindungsnetzes

Zunächst soll geklärt werden, ob die Postfach- und Kommunikationsinfrastruktur auf die in Art. 91c Abs. 4 GG enthaltenen Regelungen zum „Verbindungsnetz" gestützt werden könnte.

In Art. 91c Abs. 4 GG heißt es wörtlich:

> *[1]Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. [2]Das Nähere zur Errichtung und zum Betrieb des Verbindungsnetzes regelt ein Bundesgesetz mit Zustimmung des Bundesrates.*

Art. 91c Abs. 4 Satz 1 GG begründet eine **Verwaltungskompetenz des Bundes** hinsichtlich der Errichtung eines Verbindungsnetzes, auch „Koppelnetz" genannt. Auch wenn der Wortlaut in Art. 91c Abs. 4 Satz 1 GG ausdrücklich nur auf die **Errichtung** beschränkt ist, kann davon ausgegangen werden, dass die Verwaltungskompetenz auch den **Betrieb** des Verbindungsnetzes umfasst.[81] Hierfür spricht der systematische Zusammenhang zu Art. 91c Abs. 4 Satz 2

[81] Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 21-23.

GG, der dem Bund eine **ausschließliche Gesetzgebungskompetenz** für die Ausgestaltung von Errichtung *und* Betrieb des Verbindungsnetzes zuordnet.[82]

Die Verwaltungskompetenz gemäß Art. 91c Abs. 4 GG ist jedoch auf den Gegenstand des „Verbindungsnetzes" beschränkt. Für die darüber hinaus gehenden, an das Verbindungsnetz anzuschließenden Netze verbleibt die Zuständigkeit bei den jeweiligen Hoheitsträgern – Bund und Ländern.[83]

Laut der Gesetzesbegründung zu Art. 91c Abs. 4 GG räumt die Norm dem Bund die Aufgabe ein, „mit dem Verbindungsnetz eine sichere Plattform für den bund-/länderübergreifenden Datenaustausch zu errichten, die auch von den Ländern für den länderübergreifenden Datenaustausch genutzt werden kann".[84] Ziel sei es, „dauerhaft und sicher die gegenseitige Erreichbarkeit aller Einrichtungen der öffentlichen Verwaltung unmittelbar oder mittelbar über das Verbindungsnetz und die daran angeschlossenen Netze von Bund und Ländern zu ermöglichen" und „zudem die Verbindung der deutschen Verwaltungsnetze mit den Netzen der EU sicherstellen".[85]

Eine Definition für den **Begriff des Verbindungsnetzes** enthält das GG allerdings nicht.

Zur Ausführung von Art. 91c Abs. 4 GG hat der Bundesgesetzgeber das Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG)[86] verabschiedet und den Begriff darin – in § 2 Abs. 2 IT-NetzG – wie folgt definiert:

> *[1]Verbindungsnetz im Sinne dieses Gesetzes ist das informationstechnische Netz, welches die informationstechnischen Netze des Bundes und der Länder*

---

82 Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 46 und 48; Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 21-23.

83 Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 22.

84 Begründung zu Art. 91c Abs. 4 GG, Gesetzentwurf der Fraktionen der CDU/CSU und SPD, BT-Drucksache 16/12410 vom 24.03.2009, S. 9.

85 Ebd., S. 9 f.

86 Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG), Art. 4 des Begleitgesetzes zur zweiten Föderalismusreform vom 10. August 2009, BGBl. 2009 I S. 2702, 2706, zuletzt geändert durch Art. 3 des Gesetzes vom 19. Juli 2024, BGBl. 2024 I Nr. 245.

> *verbindet. [2]Die Übergabepunkte zu den jeweils verbundenen Netzen werden gemeinsam vereinbart.*

Der einfachgesetzlichen Legaldefinition vorangestellt hat der Bundesgesetzgeber in § 2 Abs. 1 IT-NetzG a.F.[87] zudem erläutert, was im Sinne des IT-NetzG unter „informationstechnischen Netzen" zu verstehen ist:

> *[1]Informationstechnische Netze im Sinne dieses Gesetzes sind die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, die die Übertragung von Signalen ermöglichen. [2]Ausgenommen sind Telemedien, Rundfunk sowie Sprechfunk- und Telefonnetze.*

Unabhängig von der Frage, ob diese Definition eins zu eins für die grundgesetzliche Auslegung übernommen werden kann, kommt hier jedoch ein Kernbestandteil der Definition des Verbindungsnetzes zum Ausdruck, der auch Art. 91c Abs. 4 GG sowohl nach seinem Wortlaut als auch nach seinem Sinn und Zweck entnommen werden kann: Adressiert wird durch den Begriff jedenfalls ein Datenaustausch, der **innerhalb der staatlichen Sphäre** verbleibt. Demgegenüber zielt die Schaffung einer einheitlichen föderalen Postfach- und Kommunikationsinfrastruktur auf die Kommunikation zwischen Bürgern bzw. privaten Organisationseinheiten und öffentlichen Stellen ab und geht damit über eine bund-/länderübergreifende Vernetzung öffentlicher Einrichtungen (bzw. mit Einrichtungen der EU) hinaus. Das bedeutet demnach, dass selbst für den Fall, dass eine Postfach- und Kommunikationsinfrastruktur aus informationstechnischer Sicht grundsätzlich vertretbar unter den Begriff des „Verbindungsnetzes" subsumiert werden könnte, das hier gegenständliche IT-Infrastrukturvorhaben insofern eine von Art. 91c Abs. 4 GG abweichende Zielrichtung des Datenaustauschs verfolgt. Art. 91c Abs. 4 GG kann das beschriebene Vorhaben daher aus unserer Sicht auch nicht als Ermächtigungsgrundlage tragen.

[87] § 2 Abs. 1 Satz 2 IT-NetzG wurde mit Wirkung zum 14.05.2024 dahingehend geändert, dass anstelle der „*Telemedien*" nunmehr „*digitale Dienste nach § 1 Absatz 4 Nummer 1 des Digitale-Dienste-Gesetzes*" ausgenommen sind.

Folgerungen für die Machbarkeit von ZaPuK

Art. 91c Abs. 4 GG kann nicht als Rechtsgrundlage für die Regelung und Umsetzung von ZaPuK dienen; sie könnte allenfalls ergänzend als Grundlage für rein interne, dem Datenaustausch zwischen staatlichen Einheiten dienenden Komponenten herangezogen werden.

2.2.2. Bundeskompetenz nach Art. 91c Abs. 5 GG – Regelung des informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern

Fraglich ist, ob bzw. inwieweit Art. 91c Abs. 5 GG eine geeignete Rechtsgrundlage für ZaPuK darstellen könnte. Anders als der vorangegangene Absatz befasst sich die Norm mit der Schnittstelle zwischen Verwaltung und Bürger:[88]

> *Der übergreifende informationstechnische Zugang zu den Verwaltungsleistungen von Bund und Ländern wird durch Bundesgesetz mit Zustimmung des Bundesrates geregelt.*

Mit dem Zugang zu den Verwaltungsleistungen wird die Brücke zwischen den Bürgern bzw. Unternehmen auf der einen Seite und der Verwaltung auf der anderen Seite geschlagen.[89]

Die Verfassungsnorm, um die Art. 91c GG im Jahr 2017 ergänzt worden ist,[90] begründet eine ausschließliche Gesetzgebungskompetenz des Bundes im Sinne des Art. 71 GG zur Regelung des übergreifenden informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern und ausweislich des indikativ gefassten Wortlauts insoweit auch einen Verfassungsauftrag. Diesem Auftrag ist der Bundesgesetzgeber mit dem die Verfassungsänderung im Jahr 2017 begleitenden Gesetz zur Neuregelung des bundesstaatlichen Finanzausgleichssystems ab dem Jahr 2020 und zur Änderung haushaltsrechtlicher Vorschriften und dem darin

[88] Vgl. M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 53.

[89] Mario Martini/Cornelius Wiesner, Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung Quantensprung oder zu kurz gesprungen?, Typoskript im Sinne des § 38 Abs. 4 UrhG; das Original ist abgedruckt in der ZG 32 (2017), S. 193 ff., S. 9.

[90] Abs. 5 angefügt mit Wirkung vom 20.07.2017 durch Gesetz vom 13.7.2017, BGBl. 2017 I S. 2347.

als Art. 9 enthaltenen Onlinezugangsgesetz (erste Fassung im Folgenden: OZG 1.0)[91] nachgekommen.[92]

a) Reichweite und Grenzen der Ermächtigung

Im Folgenden sollen die Reichweite und die Grenzen von Art. 91c Abs. 5 GG näher beleuchtet werden. Hierzu soll zum einen geklärt werden, welche staatlichen Maßnahmen unter den Begriff der „Verwaltungsleistung" fallen und damit der Regelungskompetenz von Art. 91c Abs. 5 GG unterliegen (Punkt aa)). Zum anderen soll geprüft werden, wie weitreichend der Begriff des „übergreifenden informationstechnischen Zugangs" zu verstehen ist und ob dieser so weit ausgelegt werden kann, dass auch eine Postfach- und Kommunikationsinfrastruktur darunter gefasst werden kann (Punkt bb)). Ferner soll untersucht werden, ob Art. 91c Abs. 5 GG den Bund auch dazu ermächtigt, zugangsbezogene Regelungen mit Bindungswirkung gegenüber den Kommunen zu erlassen (Punkt cc)).

aa) Begriff der „Verwaltungsleistungen" in Art. 91c Abs. 5 GG

Für den in Art. 91c Abs. 5 GG enthaltenen Begriff der **„Verwaltungsleistungen"** findet sich im GG keine Legaldefinition. Er wurde auch in der Gesetzesbegründung zu Art. 91c Abs. 5 GG nicht näher konkretisiert, sondern im Verfahren der Grundgesetzänderung vielmehr vorausgesetzt.[93]

Erfasst sind jedenfalls **Maßnahmen der Leistungsverwaltung**, die die Verwaltung als Teil ihres staatlichen Handlungsauftrags für Bürger oder Unternehmen – etwa im Rahmen von Antrags-, Anzeige und Genehmigungsverfahren – vorhält.[94]

---

[91] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), Art. 9 des Gesetzes zur Neuregelung des bundesstaatlichen Finanzausgleichssystems ab dem Jahr 2020 und zur Änderung haushaltsrechtlicher Vorschriften vom 14.08.2017, BGBl. 2017 I S. 3122, 3138.

[92] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 52-54.; Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c GG, Rn. 31.

[93] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 57.

[94] Vgl. M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 67.

In der Literatur wird zum Teil unter Verweis auf den Wortlaut von Art. 91c Abs. 5 GG (Verwaltungs**leistungen**) vertreten, dass **Maßnahmen der Eingriffsverwaltung** hingegen nicht unter die Bestimmung zu subsumieren seien.[95]

Die allgemeinen kompetenzrechtlichen Normen des GG (Art. 30, 83 ff. GG) treffen in ihrer Kompetenzzuweisung allerdings keine Unterscheidung nach den Bereichen der Leistungs- und Eingriffsverwaltung. Es ist auch nicht erkennbar, dass der verfassungsändernde Gesetzgeber bei der Einführung von Art. 91c Abs. 5 GG solche Verwaltungsmaßnahmen, die zwar zur digitalen Abwicklung geeignet sind, aber eine belastende Wirkung haben, prinzipiell vom übergreifenden informationstechnischen Zugang ausschließen wollte.

Da es sich bei der Grundgesetzänderung und dem Erlass des OZG 1.0 um „parallel laufende Gesetzgebungsverfahren" handelte, können Art. 91c Abs. 5 GG und das OZG 1.0 als „normatives Gesamtpaket" begriffen werden, das in seiner Gesamtheit auf einheitliche inhaltliche Vorstellungen zurückgeht. Auch wenn das einfachgesetzliche OZG 1.0 nicht unmittelbar zur Auslegung der Grundgesetznorm herangezogen werden kann – die einfachgesetzlichen Bestimmungen sind vielmehr an den Normen des GG zu messen –, sind vor diesem Hintergrund die darin zum Ausdruck gekommenen Erwägungen dennoch für die Auslegung des Verfassungsrechts beachtlich. Insbesondere für den Begriff der Verwaltungsleistungen bietet es sich daher an, sich bei der Auslegung an den Bestimmungen des OZG 1.0 zu orientieren.[96]

In § 2 Abs. 3 des OZG 1.0 wurde der Begriff wie folgt legaldefiniert:

> *„Verwaltungsleistungen" im Sinne dieses Gesetzes sind die elektronische Abwicklung von Verwaltungsverfahren und die dazu erforderliche elektronische*

[95] Vgl. M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 67.

[96] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 57; so auch Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c GG, Rn. 23.

Information des Nutzers und Kommunikation mit dem Nutzer über allgemein zugängliche Netze.[97]

Die Begriffsdefinition im OZG 1.0 knüpft also an die elektronische Abwicklung von Verwaltungsverfahren an. Aus der Gesetzesbegründung zum OZG 1.0 geht hervor, dass damit Verwaltungsverfahren im Sinne von § 9 Verwaltungsverfahrensgesetz des Bundes (VwVfG) und der entsprechenden Vorschriften der Verwaltungsverfahrensgesetze der Länder gemeint sind.[98] Eine Beschränkung auf den Bereich der bloßen Leistungsverwaltung nimmt die Begriffsdefinition im OZG 1.0 dabei nicht vor.

Überzeugend erscheint es vor diesem Hintergrund, auch im Rahmen des Art. 91c Abs. 5 GG auf die elektronische Abwicklung **aller** staatlichen Maßnahmen abzustellen, die Gegenstand eines solchen Verwaltungsverfahrens im Sinne von § 9 VwVfG und der entsprechenden Landesnormen sein können. Unter einem Verwaltungsverfahren im Sinne von § 9 VwVfG ist die nach außen wirkende Tätigkeit der Behörden zu verstehen, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrags gerichtet ist – einschließlich des Erlasses des Verwaltungsaktes oder des Abschlusses des öffentlich-rechtlichen Vertrags selbst. Erfasst von Art. 91c Abs. 5 GG sind nach der hier vertretenen Auffassung damit nicht nur begünstigende Maßnahmen der Leistungsverwaltung, sondern auch belastende Maßnahmen aus dem Bereich der Eingriffsverwaltung.

Nicht erfasst sind jedoch Maßnahmen anderer Staatsgewalten, also etwa Handlungen der Judikative und der Legislative.[99] Ebenso wenig dürften rein verwaltungsinterne Vorgänge ohne

---

[97] In der aktuellen Fassung von § 2 Abs. 3 OZG 2.0 bezieht sich die Legaldefinition nunmehr auf „Elektronische Verwaltungsleistungen". In der entsprechenden Gesetzesbegründung wird darauf hingewiesen, dass die Begriffsdefinition im Sinne einer stringenten Verwendung angepasst worden sei. Der Begriff der Verwaltungsleistung als solcher beziehe sich auf die allgemeine Definition von Verwaltungsleistung, unabhängig vom Weg der Abwicklung. Neu sei dagegen die „elektronische Verwaltungsleistung", die hier definiert wird, siehe Begründung zu § 2 Abs. 3 OZG 2.0, Gesetzesentwurf der Bundesregierung, BT-Drucksache 20/8093 vom 23.08.2023, S. 36.

[98] Begründung zum OZG 1.0, Gesetzesentwurf der Bundesregierung, BR-Drucksache 814/16 vom 30.12.16, S. 87.

[99] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 67.

Bezug zu einem konkreten Verwaltungsverfahren, einschließlich verwaltungsorganisatorischer Abläufe, unter Art. 91c Abs. 5 GG fallen. Dies gilt darüber hinaus auch für Verwaltungsleistungen, die zwar unter § 9 VwVfG zu subsumieren sind, aber naturgemäß nicht über das Internet abgewickelt werden könnten, wie etwa Realhandlungen.[100]

bb) Begriff des „übergreifenden informationstechnischen Zugangs" in Art. 91c Abs. 5 GG

In Art. 91c Abs. 5 GG nicht näher präzisiert ist ferner, was unter dem Begriff des „übergreifenden informationstechnischen Zugangs" zu verstehen ist und wie weit dieser reicht.

In der Gesetzesbegründung zu Art. 91c Abs. 5 GG spiegelt sich hinsichtlich des informationstechnischen Zugangs nicht nur ein abstraktes Konzept, sondern bereits ein konkretes Begriffsverständnis im Sinne eines **„Portalverbunds"** wider, der die jeweils fortbestehenden Verwaltungsportale verknüpfen und damit den Zugriff auf die dort digital angebotenen Verwaltungsleistungen der unterschiedlichen Verwaltungsebenen in einer zentralen Anlaufstelle bündeln soll.[101] In der Gesetzesbegründung heißt es hierzu:

> *„Die Ergänzung des Artikels 91c um einen neuen Absatz 5 dient der Umsetzung der politischen Vorgabe, den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern (einschließlich Kommunen) zu ermöglichen. […] Die Gesetzgebungsbefugnis umfasst die Errichtung dieses Portalverbundes und die grundsätzliche Pflicht zur auch elektronischen Bereitstellung von Verwaltungsleistungen des Bundes und der Länder über ihre jeweiligen Verwaltungsportale und deren Verknüpfung zu dem deutschlandweiten Portalverbund."*[102]

---

[100] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 67 f.; Ruge, in: Schmidt-Bleibtreu, Grundgesetz, Kommentar, Hofmann/Hennecke (Hrsg.), 15. Auflage, Art. 91c, Rn. 49; vgl. auch Begründung zum OZG 1.0, Gesetzesentwurf der Bundesregierung, BR-Drucksache 814/16 vom 30.12.16, S. 87.

[101] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 54.

[102] Begründung zu Art. 91c Abs. 5, Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 16.

In § 1 Abs. 2 OZG 1.0 wurde dementsprechend einfachgesetzlich eine Verpflichtung von Bund und Ländern normiert, ihre Verwaltungsportale miteinander zu einem Portalverbund zu verknüpfen. Nach der in § 2 Abs. 1 OZG 1.0 enthaltenen – jedoch wenig aussagekräftigen – Legaldefinition handelt es sich dabei um eine *technische Verknüpfung* der Verwaltungsportale von Bund und Ländern, über den der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird.

Fraglich ist vor diesem Hintergrund, ob der Begriff „Zugang" im Sinne von Art. 91c Abs. 5 GG auch eine Postfach- und Kommunikationslösung zwischen Privaten und der Verwaltung trägt und ob der Bund auf dieser Basis auch die Zurverfügungstellung einer entsprechenden IT-Infrastruktur regeln kann.

(1) Postfach- und Kommunikationsinfrastruktur als „informationstechnischer Zugang"

Der Wortlaut schließt ein solches Verständnis jedenfalls nicht *per se* aus. Der Bedeutungsgehalt des Begriffs „Zugang" lässt – ausgehend vom allgemeinen Sprachgebrauch – jedenfalls die Möglichkeit eines weit gefassten Verständnisses zu. Danach kann das Wort „Zugang" zum einen eine „Stelle" oder einen „Weg, der in einen Raum, Ort hineinführt", zum anderen das „Betreten" bzw. „Hineingehen" bezeichnen.[103] Diese Bedeutungsfacetten legen bereits nahe, dass „Zugang" nicht nur zwingend eine punktuelle Eintrittsmöglichkeit erfasst, sondern allgemein den eröffnenden Weg zu einem Zielbereich beschreibt. Hinzu kommt, dass der Begriff im EDV-Bereich auch die Bedeutung eines „Accounts"[104] trägt, also einer technisch vermittelten Zugriffsmöglichkeit auf digitale Systeme und Kommunikationsräume. Von diesem Verständnis ausgehend erscheint auch eine infrastrukturelle Anbindung für eine Kommunikations- bzw. Postfachlösung sprachlich noch mit dem Begriff des „Zugangs" vereinbar. Denn eine solche Infrastruktur bildet einen Kanal im Sinne eines dauerhaft bestehenden Zugangswegs, über den die Bürger oder Unternehmen die Verwaltung fortlaufend erreichen können und über den ein wechselseitiger Kontakt stattfinden kann.

[103] Siehe https://www.duden.de/rechtschreibung/Zugang, zuletzt abgerufen am 09.12.2025.
[104] Siehe ebd.

Dafür, dass der „Zugang" im Sinne von Art. 91c Abs. 5 GG auch einen Kommunikationskanal zwischen Bürgern/Unternehmen und der Verwaltung (mit-)umfassen können sollte, spricht auch die Gesetzesbegründung von Art. 91c Abs. 5 GG, die mitunter auch auf die Kommunikation bei der Nutzung des Portalverbundes eingeht. Hierin heißt es:

> *„Um eine medienbruchfreie Kommunikation bei der Nutzung dieses Portalverbundes und der hierüber angebotenen Leistungen sowie Kompatibilität zu anderen gesetzlich vorgesehenen Zugängen zur Verwaltung zu gewährleisten, müssen für die elektronische Abwicklung von Verwaltungsleistungen über den Portalverbund einheitliche Vorgaben für IT-Anwendungen, die Kommunikation und die Sicherheit gelten. Diese kann der Bund auf der Grundlage der Gesetzgebungskompetenz in Absatz 5 mit Zustimmung des Bundesrates vorgeben."*[105]
>
> (Hervorhebung hier hinzugefügt)

Ferner lässt sich in diesem Zusammenhang auch auf die einfachgesetzliche Ausgestaltung des OZG 1.0 und die dazugehörigen Gesetzesmaterialien verweisen. Denn das OZG 1.0 sah bereits ein einheitliches Identitätsmanagement über Nutzerkonten vor (§§ 2 Abs. 5, 3 Abs. 2 OZG 1.0), wozu auch der Zugriff auf ein digitales Postfach zählte. Zwar findet dieses im OZG 1.0 keine ausdrückliche Erwähnung, sollte jedoch ausweislich der Gesetzesmaterialien in der Bestimmung des § 8 Abs. 3 OZG 1.0 angelegt sein, die es gestattet, mit Einwilligung des Nutzers im Nutzerkonto elektronische Dokumente zu Verwaltungsvorgängen sowie Status- und Verfahrensinformationen innerhalb des Nutzerkontos zu speichern und zu verarbeiten.[106]

Zum Teil wird eingewandt, die systematische Stellung des Art. 91c Abs. 5 GG in dem durch Kooperationsbestimmungen geprägten Abschnitt VIIIa des GG spreche eher für eine restriktive

[105] Begründung zu Art. 91c Abs. 5, Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 16 f.

[106] Mario Martini/Cornelius Wiesner, Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung Quantensprung oder zu kurz gesprungen?, Typoskript im Sinne des § 38 Abs. 4 UrhG; das Original ist abgedruckt in der ZG 32 (2017), S. 193 ff., S. 17.

Auslegung der Kompetenznorm; eine in diesem Abschnitt angesiedelte ausschließliche Gesetzgebungskompetenz des Bundes sei nur punktuell zu verstehen.[107]

Jedoch zielt Art. 91c Abs. 5 GG erkennbar auf die Regelung einer einheitlichen digitalen Eingangsschnittstelle zu den Verwaltungsverfahren von Bund und Ländern ab. Da sich ein übergreifender digitaler Zugang zu Verwaltungsleistungen aber nur dann funktionsgerecht gewährleisten lässt, wenn er medienbruchfrei ausgestaltet ist und sich nicht nur – rein punktuell – im erstmaligen Betreten der digitalen Verwaltungsplattform des zuständigen Hoheitsträgers erschöpft, ist davon auszugehen, dass er auch die Ausgestaltung solcher IT-Infrastrukturen erfasst, die den Nutzer und die Behörde während der Durchführung des Verwaltungsverfahrens miteinander in Kontakt hält und dem Nutzer das fortwährende Ansteuern der Verwaltungsleistung ermöglicht. Dies schließt auch den „Zugang" des Nutzers zu der abschließenden behördlichen Entscheidung mit ein.[108]

Auch wenn der verfassungsändernde Gesetzgeber bei der Schaffung des Art. 91c Abs. 5 GG bereits konkret die Herstellung eines Portalverbunds vor Augen hatte und der einfache Gesetzgeber mit seiner Regelung durch das OZG 1.0 bereits von der Kompetenznorm Gebrauch gemacht hat, ist Art. 91c Abs. 5 GG nach seiner verfassungsrechtlichen Ausgestaltung nicht zwingend auf eine entsprechende Auslegung beschränkt. Vielmehr ist auch eine Auslegung möglich, nach der der übergreifende informationstechnische Zugang eine informationstechnische Postfach- und Kommunikationslösung im Verhältnis zwischen den Bürgern/Unternehmen und der Verwaltung erfasst und eine – ggf. von den Bestimmungen des OZG 1.0 bzw. deren späteren Änderungen[109] losgelöste – bundesrechtliche Regelung hierüber ermöglicht. Wenn der Bund den informationstechnischen Zugang zu den Verwaltungsleistungen regeln darf, darf er auch eine Regelung über die Zurverfügungstellung der dafür als direktes Element

[107] Mario Martini/Cornelius Wiesner, Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung Quantensprung oder zu kurz gesprungen?, Typoskript im Sinne des § 38 Abs. 4 UrhG; das Original ist abgedruckt in der ZG 32 (2017), S. 193 ff., S. 13.

[108] Ebd., S. 18 f.

[109] Art. 1 des Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz — OZGÄndG), BGBl. 2024 I Nr. 245 vom 23.07.2024.

erforderlichen IT-Infrastruktur treffen.[110] Gesetzestechnisch ist sowohl denkbar, dies über eine Anpassung des bestehenden OZG umzusetzen, als auch zu diesem Zweck ein separates Bundesgesetz zu erlassen.

(2) Mögliche Grenzen der kompetenziellen Reichweite („Frontend" versus „Backend")

In der Literatur wird insbesondere im Zusammenhang mit der Diskussion um den zum 1. Februar 2026 in Kraft getretenen NOOTS-Staatsvertrag[111] zum Teil vertreten, Art. 91c Abs. 5 GG ermächtige den Bund lediglich zu Entscheidungen über das sog. „Frontend", während ihm regulatorische Maßnahmen im „Backend" aber *generell verwehrt* seien.[112]

Eine derart schematische Unterscheidung lässt sich Art. 91c Abs. 5 GG jedoch nicht ohne Weiteres entnehmen. Die Vorschrift ermächtigt den Bund zur Regelung des „übergreifenden informationstechnischen Zugangs" zu den Verwaltungsleistungen von Bund und Ländern. Weder verwendet sie die Begriffe des Front- oder Backends noch beschränkt sie die Regelungskompetenz auf bestimmte technische Architekturebenen. Maßgeblich dürfte daher weniger die technische Einordnung einzelner Komponenten, sondern vielmehr deren funktionale Bedeutung für die Herstellung des informationstechnischen Zugangs sein.

Danach sprechen die besseren Argumente dafür, die vorgesehene Postfach- und Kommunikationsinfrastruktur insgesamt dem informationstechnischen Zugang zuzuordnen. Anders als das NOOTS zielt das Vorhaben nicht lediglich auf den behördenübergreifenden Datenaustausch ab, sondern auf die Bereitstellung einer Kommunikationsschnittstelle zwischen Privaten und der Verwaltung (siehe hierzu die Ausführungen zu Art. 91c Abs. 4 GG unter Punkt 2.2.1). Die

[110] Vgl. Mario Martini/Cornelius Wiesner, Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung Quantensprung oder zu kurz gesprungen?, Typoskript im Sinne des § 38 Abs. 4 UrhG; das Original ist abgedruckt in der ZG 32 (2017), S. 193 ff., S. 19, die dies bzgl. der durch das OZG 1.0 geregelten Nutzerkonten mit Postfach und Cloud als Elemente des Zugangs feststellen.

[111] Vertrag über die Errichtung, den Betrieb und die Weiterentwicklung des Nationalen Once-Only-Technical-Systems (NOOTS) – Vertrag zur Ausführung von Artikel 91c Absatz 1, Absatz 2 GG – NOOTS-Staatsvertrag, BGBl. 2025 I Nr. 325, S. 3; 2026 I Nr. 35.

[112] Martini/Botta: Government-as-a-Platform - Vorschlag einer Änderung des Grundgesetzes zur Staatsmodernisierung, NJW 2025, 1464 (1467 f.), Rn. 32.

Infrastruktur – einschließlich Frontends und Backends – dient dabei der medienbruchfreien Übermittlung von Nachrichten und Dokumenten sowie der Durchführung der digitalen Kommunikation unabhängig vom jeweils betroffenen Fachverfahren. Nach der derzeitigen Konzeption greift sie weder in die fachliche Entscheidung noch in die Bearbeitung der Verwaltungsverfahren ein. Zwar soll der Bund eine einheitliche Infrastruktur einschließlich zentral bereitgestellter Backendkomponenten vorgeben; zugleich soll jedoch der Betrieb eigener dezentraler Backendlösungen möglich bleiben, sofern diese die vorgegebenen technischen Anschluss- und Interoperabilitätsanforderungen erfüllen. Den Ländern (und Kommunen) verbleibt damit ein erheblicher Gestaltungsspielraum hinsichtlich der Ausgestaltung ihrer internen informationstechnischen Systeme und Fachverfahren. Vor diesem Hintergrund sprechen überwiegende Gründe dafür, dass eine derart begrenzte Regelung von Art. 91c Abs. 5 GG umfasst ist.

cc) Bindungswirkung gegenüber den Kommunen

Fraglich ist, ob über Art. 91c Abs. 5 GG die Errichtung von ZaPuK auch insoweit geregelt werden kann, als der Anschluss und Verwaltungsverfahren der Kommunen betroffen sind.

In der Rechtsliteratur ist umstritten, ob der Bund auf Basis von Art. 91c Abs. 5 GG auch den digitalen Zugang zu den auf kommunaler Ebene erbrachten Verwaltungsleistungen verbindlich regeln kann: Zum Teil wird vertreten, dass der Bund aus Art. 91c Abs. 5 GG keine Regelungsbefugnis herleiten könne, die es ihm erlauben würde, die Kommunen unmittelbar legislativ zu binden. Die Kommunen seien danach lediglich mittelbar – über die Länder – einbezogen. Diese hätten die Pflichten, die ihnen auf Basis von Art. 91c Abs. 5 GG einfachgesetzlich auferlegt würden, an ihre mittelbare Staatsverwaltung weiterzureichen.[113] Andere Literaturstimmen sprechen sich demgegenüber zugunsten einer Einbeziehung der Kommunen in die durch Art. 91c Abs. 5 GG begründete Regelungskompetenz aus.[114]

[113] Siehe etwa M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 63 bis 66.

[114] Siehe etwa Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 66 bis 71; Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 34.

Aus der Auslegung der Regelung unter Berücksichtigung von Wortlaut, Entstehungsgeschichte, Systematik und Sinn und Zweck ergeben sich unserer Auffassung nach überwiegende Gründe für eine Einbeziehung der kommunalen Ebene in eine verbindliche Regelung des digitalen Zugangs auf Grundlage von Art. 91c Abs. 5 GG – jedenfalls dann, wenn bestimmte Grenzen beachtet werden. Im Einzelnen:

(1) Wortlaut von Art. 91c Abs. 5 GG

Der Wortlaut von Art. 91c Abs. 5 GG adressiert die „Verwaltungsleistungen von Bund und Ländern". Gemeinden oder Gemeindeverbände werden in der Bestimmung dagegen nicht ausdrücklich erwähnt. Allerdings bezeichnet der Begriff der „Länder" im Staatsorganisationsrecht regelmäßig nicht nur die Landesebene im engeren Sinne, sondern schließt die Kommunen als Teil der mittelbaren Landesverwaltung mit ein. Auch der Umstand, dass das GG an anderer Stelle – etwa in Art. 106 GG hinsichtlich der Steuerertragsverteilung – ausdrücklich zwischen Ländern und Gemeinden differenziert, rechtfertigt noch keinen gegenteiligen Schluss. Die gesonderte Erwähnung der Gemeinden kann vielmehr den Besonderheiten der jeweiligen Regelungsmaterie geschuldet sein und einer gezielten Abgrenzung zu den Ländern dienen. Der Wortlaut des Art. 91c Abs. 5 GG steht demnach einer Einbeziehung der Kommunen nicht entgegen.[115]

(2) Entstehungsgeschichte

Die Entstehungsgeschichte des Art. 91c Abs. 5 GG spricht eher für eine Einbeziehung der Kommunen.[116] Die Begründung des Gesetzesentwurfs zur Grundgesetzänderung verdeutlicht, dass der verfassungsändernde Gesetzgeber einen gebietskörperschaftsübergreifenden digitalen Zugang zu Verwaltungsleistungen schaffen wollte, der die kommunale Ebene miteinschließt.

Die Materialien der Bundesregierung zur Grundgesetzänderung sowie die Begründung des Begleitgesetzes sprechen wiederholt von den Verwaltungsleistungen/Behörden/Portalen „von Bund und Ländern (einschließlich Kommunen)" und beschreiben das Ziel eines bundesweiten

[115] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 66.
[116] Ebd., Rn. 67.

Portalverbunds, über den Nutzerinnen und Nutzer auf die Online-Verwaltungsleistungen von Bund, Ländern und Kommunen zugreifen können.[117]

Im Gesetzgebungsverfahren zum Begleitgesetz vertrat der Bundesrat demgegenüber – unter Hinweis auf das Durchgriffsverbot des Art. 84 Abs. 1 Satz 7 GG – noch die Auffassung, dass den Kommunen durch das OZG 1.0 weder unmittelbar Pflichten auferlegt noch die Länder verpflichtet würden, entsprechende Verpflichtungen landesgesetzlich an die Kommunen weiterzugeben. Der Bundesrat schlug daher vor, ausdrücklich zu regeln, dass Gemeinden und Gemeindeverbände dem Portalverbund lediglich freiwillig beitreten können. Zur Begründung verwies er insbesondere darauf, dass in der Besprechung der Regierungschefinnen und Regierungschefs von Bund und Ländern Einigkeit bestanden habe, dass die Errichtung des Portalverbunds nicht zu einer Mitverpflichtung der Kommunen führen dürfe. Zugleich betonte der Bundesrat jedoch, dass die Infrastruktur des Portalverbunds so auszugestalten sei, dass ein freiwilliger Beitritt der Kommunen jederzeit möglich ist.[118]

Die Bundesregierung trat dieser Auffassung ausdrücklich entgegen. Die Wirksamkeit des Gesetzesvorhabens hänge maßgeblich auch von der Einbeziehung der Gemeinden und Gemeindeverbände ab, da ein Großteil der Verwaltungsleistungen auf kommunaler Ebene angeboten werde und diese in der Regel die erste Anlaufstelle der Bürgerinnen und Bürger sei. Bei den Kommunen handele es sich verfassungsrechtlich um einen Teil der Länder. Das Aufgabenübertragungsverbot des Art. 84 Abs. 1 Satz 7 GG sei nicht berührt, da es nicht um die Übertragung neuer Verwaltungsaufgaben gehe, sondern nur die Art und Weise der Erfüllung bestehender Verwaltungsaufgaben geregelt werde.[119]

[117] Begründung zu Art. 91c Abs. 5, Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 12 und 16; Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11135 vom 13.02.2017, S. 5 und 91.

[118] Stellungnahme des Bundesrats, Anlage 3 des Gesetzesentwurfs der Bundesregierung, BT-Drucksache 18/11135 vom 13.02.2017, S. 138 f.

[119] Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates, Drucksache 18/11185 vom 15.02.2017, S. 6.

Der Bundesrat stimmte dem OZG 1.0 letztlich zu, ohne dass eine Ausnahmeregelung für die Kommunen in den Gesetzestext aufgenommen worden wäre, und ließ das „normative Gesamtpaket" im Ergebnis jedenfalls nicht hieran scheitern.[120]

(3) Systematik

Auch die systematische Stellung des Art. 91c Abs. 5 GG spricht dafür, dass die Norm grundsätzlich eine Einbeziehung der kommunalen Ebene ermöglicht.

Zwar gewährleisten Art. 28 Abs. 2 GG und das in Art. 84 Abs. 1 Satz 7 sowie Art. 85 Abs. 1 Satz 2 GG verankerte Durchgriffsverbot die Eigenständigkeit der kommunalen Ebene (siehe hierzu Punkt 1.2.3). Art. 28 Abs. 2 GG räumt den Gemeinden und Gemeindeverbänden das Recht auf kommunale Selbstverwaltung ein und schützt insbesondere ihre Befugnis, die Angelegenheiten der örtlichen Gemeinschaft eigenverantwortlich wahrzunehmen und ihre Verwaltung organisatorisch selbst zu gestalten. Das Durchgriffsverbot untersagt dem Bundesgesetzgeber grundsätzlich, Gemeinden und Gemeindeverbänden durch Bundesgesetz Aufgaben zu übertragen. Die Bestimmungen begrenzen damit die bundesgesetzlichen Einwirkungsmöglichkeiten auf die Kommunen und sind bei der Auslegung des Art. 91c Abs. 5 GG zu berücksichtigen.

Hieraus folgt jedoch nicht, dass kommunale Verwaltungsleistungen von vornherein dem Anwendungsbereich des Art. 91c Abs. 5 GG entzogen wären. Weder Art. 28 Abs. 2 GG noch Art. 84 Abs. 1 Satz 7 bzw. Art. 85 Abs. 1 Satz 2 GG schließen bundesgesetzliche Regelungen mit Auswirkungen auf die Kommunen generell aus. Sie stehen einer Einbeziehung der Kommunen lediglich insoweit entgegen, als die bundesgesetzliche Ausgestaltung zu einer unzulässigen Aufgabenübertragung bzw. zu einer damit funktional vergleichbaren Erweiterung bestehender Aufgaben führt oder die kommunale Selbstverwaltung unverhältnismäßig beeinträchtigt.

Im Hinblick auf das Durchgriffsverbot ist zunächst davon auszugehen, dass eine auf Art. 91c Abs. 5 GG gestützte bundesgesetzliche Regelung des übergreifenden informationstechnischen Zugangs zu kommunalen Verwaltungsleistungen für sich genommen keine Aufgabenübertragung im Sinne des Art. 84 Abs. 1 Satz 7 bzw. Art. 85 Abs. 1 Satz 2 GG darstellt. Art. 91c Abs. 5

[120] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 67.

GG ermächtigt seinem Regelungsgegenstand nach lediglich dazu, die Art und Weise zu regeln, in der bereits bestehende Verwaltungsleistungen elektronisch erreichbar gemacht werden. Die den Kommunen zugewiesenen Sachaufgaben bleiben hiervon grundsätzlich unberührt; der sachliche Zuständigkeitsbereich an sich nicht erweitert. Auch die Vorgabe interoperabler Kommunikationswege oder technischer Standards führt als solche noch nicht zu einer Aufgabenübertragung.

Allerdings erschöpft sich der Schutzbereich des Durchgriffsverbots nicht in einer erstmaligen Übertragung neuer Aufgaben. Nach der Rechtsprechung des BVerfG werden auch solche Änderungen bestehender Aufgaben erfasst, die einer erstmaligen Aufgabenübertragung funktional gleichkommen (vgl. hierzu bereits die Ausführungen unter 1.2.3). Dies kann insbesondere dann der Fall sein, wenn bundesgesetzliche Vorgaben erhebliche organisatorische, personelle oder finanzielle Mehrbelastungen verursachen und dadurch die Eigenverantwortlichkeit der Kommunen in vergleichbarer Weise beeinträchtigen. Der Bundesgesetzgeber darf unter dem Deckmantel der Regelung des informationstechnischen Zugangs auf Basis von Art. 91c Abs. 5 GG daher nicht beliebige organisatorische oder technische Anforderungen an die kommunale Verwaltung stellen. Die Grenze dürfte jedenfalls dort erreicht sein, wo gesetzliche Vorgaben tiefgreifende Anpassungen der Verwaltungsorganisation erzwingen oder einen erheblichen Umstellungs- und Investitionsaufwand auslösen.

Vor diesem Hintergrund spricht viel dafür, dass eine bundesgesetzliche **Verpflichtung zum Anschluss an eine zentrale Postfach- und Kommunikationslösung** die Grenzen des Durchgriffsverbots grundsätzlich nicht überschreitet, sofern sie sich auf die Vorgabe eines einheitlichen Kommunikationskanals sowie der hierfür erforderlichen technischen Anschluss- und Interoperabilitätsanforderungen beschränkt. Denn in diesem Fall regelt das Bundesgesetz lediglich die Modalitäten des informationstechnischen Zugangs, ohne den Kommunen neue Sachaufgaben zuzuweisen oder ihre bestehenden Aufgaben in einer funktional einer Aufgabenübertragung gleichkommenden Weise zu erweitern. Dies gilt allerdings nur, soweit die Herstellung des technischen Anschlusses keinen erheblichen organisatorischen, personellen oder finanziellen Umstellungsaufwand erfordert. Führt die Anschlussverpflichtung demgegenüber zu tiefgreifenden Anpassungen der kommunalen IT- oder Verwaltungsorganisation oder macht

sie erhebliche Investitionen erforderlich, kann bereits hierin eine Belastung liegen, die einer Aufgabenübertragung funktional nahekommt. Gleiches gilt, wenn die bundesgesetzlichen Vorgaben über die Festlegung technischer Anschlussbedingungen hinausgehen und den Kommunen eigenständige Entwicklungs-, Betriebs- oder Finanzierungspflichten auferlegen. Je stärker die bundesrechtlichen Anforderungen die kommunale Organisation und Ressourcenausstattung in Anspruch nehmen, desto eher stellt sich die Frage, ob die Schwelle zu einer funktional einer Aufgabenübertragung gleichkommenden Erweiterung kommunaler Verwaltungsaufgaben überschritten wird.

Für die weitere Ausgestaltung des Vorhabens folgt hieraus, dass insbesondere die konkreten organisatorischen, personellen und finanziellen Belastungen, die den Kommunen durch die Herstellung und den Betrieb des Anschlusses an die Postfach- und Kommunikationsinfrastruktur entstehen, sorgfältig in den Blick zu nehmen sind. Die Belastung der kommunalen Ebene fällt regelmäßig geringer aus, wenn zentrale Infrastrukturkomponenten durch den Bund bereitgestellt, betrieben und finanziert werden. Umgekehrt nimmt das Risiko einer Beeinträchtigung der kommunalen Selbstverwaltung sowie einer funktional einer Aufgabenübertragung gleichkommenden Belastung zu, wenn den Kommunen erhebliche und dauerhaft zu tragende Implementierungs-, Betriebs- oder Personalkosten auferlegt werden. Eine solche Ausgestaltung könnte – abhängig von Umfang und Intensität der Belastungen – an die Grenzen dessen stoßen, was Art. 84 Abs. 1 Satz 7 und Art. 85 Abs. 1 Satz 2 GG zulassen.

Dies gilt auch mit Blick auf die in Art. 28 Abs. 2 GG allgemein geregelte Selbstverwaltungsgarantie der Kommunen. Die bundesgesetzliche Regelung darf die finanziellen und personellen Ressourcen zum einen nicht in einem Umfang in Anspruch nehmen, der die Wahrnehmung freiwilliger Selbstverwaltungsaufgaben erschwert oder unmöglich macht. Der Gesetzgeber muss den Kommunen zum anderen einen hinreichenden organisatorischen Gestaltungsspielraum belassen und darf ihre Fähigkeit, ihre Organisation an die örtlichen Gegebenheiten anzupassen, nicht entleeren. Art und Umfang der auferlegten Belastungen dürfen die Organisations-, Finanz- und Personalhoheit der Kommunen nicht erheblich beeinträchtigen.

Eine Regelung des digitalen Zugangs zu den Verwaltungsleistungen der Kommunen, die sich auf eine Standardisierung des digitalen Kommunikationsweges sowie die Festlegung technischer Schnittstellen und Anschlussbedingungen beschränkt, lässt den Kern der kommunalen Organisationsfreiheit grundsätzlich unberührt. Eine solche Regelung greift weder in die eigenverantwortliche Ausgestaltung der Fachverfahren noch die innere Verwaltungsorganisation der Kommunen ein. Positiv ist dabei insbesondere eine Ausgestaltung des digitalen Kommunikationsweges zu bewerten, die – wie nach der derzeitigen Konzeption von ZaPuK geplant – den Kommunen einerseits zentrale Komponenten der Infrastruktur zum Gebrauch bereitstellt, andererseits aber die Möglichkeit eröffnet, eigene Frontend- und Backendlösungen einzusetzen, sofern diese die vorgegebenen Anschluss- und Interoperabilitätsanforderungen erfüllen. Die verbleibende organisatorische und technische Gestaltungsfreiheit der Kommunen spricht gegen eine weitgehende bundesrechtliche Determinierung der kommunalen Aufgabenerfüllung.

Anders zu beurteilen wäre demgegenüber eine bundesgesetzliche Ausgestaltung, die den Kommunen keinen Gestaltungsspielraum mehr belässt. Problematisch wäre etwa eine Regelung, die eine ausnahmslose Verpflichtung zur Nutzung der zentralen Postfach- und Kommunikationslösung vorsieht oder den Parallelbetrieb eigener Lösungen vollständig ausschließt. In einem solchen Fall wären die Kommunen gehindert, auf örtliche Besonderheiten oder unterschiedliche tatsächliche Rahmenbedingungen – etwa einen regional unterschiedlich weit fortgeschrittenen Breitbandausbau oder bereits etablierte und von der Bevölkerung akzeptierte digitale Kommunikationslösungen – angemessen zu reagieren.

(4) Sinn und Zweck

Für eine Einbeziehung der kommunalen Ebene in den Regelungsbereich von Art. 91c Abs. 5 GG spricht schließlich der Sinn und Zweck der Norm.

Die Vorschrift zielt gerade auf die Schaffung eines verwaltungsträgerübergreifenden informationstechnischen Zugangs ab und wäre in ihrer praktischen Wirksamkeit erheblich eingeschränkt, wenn sie die kommunale Ebene, auf der ein erheblicher Teil der Verwaltungsleistungen erbracht wird, von vornherein ausnehmen würde. Die Errichtung eines umfassenden

Portalverbunds für die Angebote aller Verwaltungen kann sinnvoll nur dann bewerkstelligt werden kann, wenn auch die Verwaltungsleistungen der Kommunen integriert werden.[121]

Dies dürfte insbesondere vor dem Hintergrund gelten, dass das BVerfG in seiner Rechtsprechung das Gebot betont, dass derjenigen Auslegung einer Verfassungsnorm der Vorzug zu geben ist, die ihre Wirkungskraft am stärksten entfaltet.[122]

b) Verwaltungsvollzug und Finanzierung

Nachdem die Reichweite und die Grenzen der in Art. 91c Abs. 5 GG enthaltenen Gesetzgebungskompetenz des Bundes aufgezeigt wurden, sollen im Folgenden die Fragen des Verwaltungsvollzugs und der Finanzierung bei Nutzung des Art. 91c Abs. 5 GG als Rechtsgrundlage betrachtet werden.

Bei Erlass einer entsprechenden bundesgesetzlichen Regelung ist zu berücksichtigen, dass sich Art. 91c Abs. 5 GG seinem Wortlaut nach auf die **Begründung einer Gesetzgebungskompetenz** beschränkt. Ob aus der Vorschrift darüber hinaus auch eine auf die Herstellung des übergreifenden informationstechnischen Zugangs gerichtete Verwaltungskompetenz des Bundes abgeleitet werden kann, ist nicht abschließend geklärt.[123] Zwar scheint Art. 91c Abs. 5 GG in der Staatspraxis bereits als Grundlage für die Bereitstellung von IT-Komponenten durch den Bund herangezogen zu werden. Gemäß § 3 Abs. 1 Satz 1 OZG stellt der Bund das zentrale Bürgerkonto (DeutschlandID/BundID) bereit. Die Gesetzesbegründung verweist darauf, dass der Bund

---

[121] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 71.

[122] Siehe etwa BVerfG, Urteil vom 20.02. 2001 - 2 BvR 1444/00, NJW 2001, 1121 (1122) und Beschluss vom 07.07.2020 – 2 BvR 696/12, BeckRS 2020, 18640, Rn. 76.

[123] Vgl. etwa Kment, in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 19. Auflage 2026, Art. 91c, Rn. 7, nach dessen Auffassung Art. 91c Abs. 5 GG eine obligatorische Bundesverwaltungskompetenz für die Errichtung des bundesweiten Portalverbunds einschließlich der Verknüpfung der Verwaltungsportale von Bund und Ländern enthält; vgl. auch Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Band 3, Art. 83-146, 8. Auflage 2024, Art. 91c, Rn. 33, der aus Art. 91c Abs. 5 GG eine Verwaltungskompetenz des Bundes für den Betrieb der für den Zugang erforderlichen informationstechnischen Systeme herleitet; vgl. dagegen etwa Schulz: Eine Infrastrukturkompetenz des Bundes für die Verwaltungsdigitalisierung, RDi 2025, 207 (209), Rn. 8 ff. und Starosta: Der Portalverbund zwischen Bund und Ländern: Artikel 91c Absatz 5 GG und dessen einfachgesetzliche Ausgestaltung im verfassungsrechtlichen Wertgefüge, 1. Auflage 2022, Baden-Baden, Nomos Verlagsgesellschaft, S. 52 ff., die in der Vorschrift nur eine (ausschließliche) Gesetzgebungskompetenz des Bundes sehen.

damit die Aufgabe der sicheren Identifizierung und Authentifizierung übernehme, ohne insoweit die Frage der Verwaltungskompetenz aufzuwerfen.[124] Dogmatisch überzeugender erscheint jedoch die Einordnung von Art. 91c Abs. 5 GG als reine Gesetzgebungskompetenz. Denn im Gegensatz zu Art. 91c Abs. 4 GG, aus dessen Wortlaut („Der Bund errichtet […] Das Nähere […] regelt ein Bundesgesetz") sich die Verwaltungskompetenz eindeutig ergibt, trifft Art. 91c Abs. 5 GG („wird durch Bundesgesetz […] geregelt") keine Aussagen zum Gesetzesvollzug. Eine eigenständige Kostentragungsregel ist im Wortlaut von Art. 91c Abs. 5 GG ebenso wenig angelegt. Nach der hier vertretenen Auffassung obliegt der Vollzug eines auf Art. 91c Abs. 5 GG gestützten Bundesgesetzes daher nach der Systematik der Art. 83 ff. GG im Ausgangspunkt den Ländern,[125] die damit gemäß der allgemeinen Lastenverteilungsregel des Art. 104a Abs. 1 GG (Konnexitätsgrundsatz) grundsätzlich auch die bei ihren Behörden entstehenden Zweckausgaben und Verwaltungsausgaben zu tragen haben.

Nach der Vorstellung des verfassungsändernden Gesetzgebers 2017 sollte allerdings die Verknüpfung zu dem deutschlandweiten Portalverbund dergestalt erfolgen, dass „der Bund einen zentralen informationstechnischen Zugang zu seinen Verwaltungsleistungen (errichtet), über den auch die Länder ihre Verwaltungsleistungen elektronisch bereitzustellen haben". Die „Regelungsbefugnis" umfasse nach der Gesetzesbegründung „auch die Kostentragung für die Schnittstellen zwischen den Verwaltungsportalen von Bund und Ländern".[126] Ein solcher Ansatz kann unserer Auffassung nach auch auf die Konzeption der verfassungsrechtlichen Machbarkeit von ZaPuK übertragen werden, um insbesondere zu vermeiden, dass die Finanzierungsverantwortung in der Hauptsache bei den Ländern liegt. In Bezug auf ZaPuK ließe sich entsprechend argumentieren, dass die Kommunikationsinfrastruktur ihren Ausgangspunkt in der Bundeseigenverwaltung nimmt (Art. 86 GG) und die für ihre Errichtung anfallenden Kosten daher

[124] Vgl. Begründung zu § 3 OZG, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 23.08.2023, Drucksache 20/8093, S. 38 und 24.

[125] So auch Schulz: Eine Infrastrukturkompetenz des Bundes für die Verwaltungsdigitalisierung, RDi 2025, 207 (209), Rn. 8 ff.; Starosta: Der Portalverbund zwischen Bund und Ländern: Artikel 91c Absatz 5 GG und dessen einfachgesetzliche Ausgestaltung im verfassungsrechtlichen Wertgefüge, 1. Auflage 2022, Baden-Baden, Nomos Verlagsgesellschaft, S. 52 ff.

[126] Begründung zu Art. 91c Abs. 5, Gesetzesentwurf der Bundesregierung, BT-Drucksache 18/11131 vom 13.02.2017, S. 16.

– vorbehaltlich besonderer Regelungen – grundsätzlich vom Bund zu tragen sind (Näheres zu einer möglichen Ausgestaltung unter 2.3).[127]

Allerdings besteht auch die Möglichkeit, dass der Bund die Bereitstellung der Postfach- und Kommunikationsinfrastruktur oder jedenfalls einen Teilbereich dieser Aufgabe auf Basis von Art. 87 Abs. 3 Satz 1 GG „an sich zieht" und per Bundesgesetz auf eine neue oder bereits bestehende Verwaltungseinheit überträgt. Denn hat der Bund die Gesetzgebungskompetenz für eine bestimmte Sachmaterie inne, eröffnet ihm Art. 87 Abs. 3 GG eine Organisationsbefugnis in Bezug auf Verwaltungseinrichtungen für diese Angelegenheiten:

> *[1]Außerdem können für Angelegenheiten, für die dem Bunde die Gesetzgebung zusteht, selbständige Bundesoberbehörden und neue bundesunmittelbare Körperschaften und Anstalten des öffentlichen Rechtes durch Bundesgesetz errichtet werden. [2]Erwachsen dem Bunde auf Gebieten, für die ihm die Gesetzgebung zusteht, neue Aufgaben, so können bei dringendem Bedarf bundeseigene Mittel- und Unterbehörden mit Zustimmung des Bundesrates und der Mehrheit der Mitglieder des Bundestages errichtet werden.*

Die Errichtung von Behörden und Verwaltungsträgern im Sinne des Art. 87 Abs. 3 Satz 1 GG umfasst sowohl deren Gründung und Ausgestaltung als auch die Festlegung ihrer Aufgaben und Befugnisse. Anerkannt ist, dass auf Basis von Art. 87 Abs. 3 Satz 1 GG Aufgaben auch auf bereits *bestehende* Verwaltungseinheiten[128] übertragen werden können.[129] Nach der Rechtsprechung des BVerfG enthält Art. 87 Abs. 3 Satz 1 GG eine Kompetenzregelung, die im Sinne

[127] Vgl. auch Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 75.

[128] Auf Grundlage von Art. 87 Abs. 3 Satz 1 GG können Aufgaben nicht nur auf selbständige Bundesoberbehörden, sondern auch auf bundesunmittelbare Körperschaften und Anstalten des öffentlichen Rechts übertragen werden. Darin ist ein allgemeiner Verweis auf die in Art. 86 Satz 1 Alt. 2 GG exemplarisch aufgezählten Formen mittelbarer Bundesverwaltung zu sehen und somit letztendlich auf alle Fälle der bundesmittelbaren Verwaltung durch mit eigener Rechtspersönlichkeit ausgestatteter Organisationseinheiten des Bundes, siehe Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 87, Rn. 47.

[129] Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 87, Rn. 52; siehe auch VG Würzburg Urteil vom 09.11.2004 – 4 K 04.948, NVwZ 2005, 471 (475); BVerwG, Urteil vom 30.06.2005 – 7 C 26/04, NVwZ 2005, 1178 (1184) und BVerfG, Beschluss vom 14.05.2007 – 1 BvR 2036/05, NVwZ 2007, 942 (944).

von Art. 83 GG etwas "anderes zulässt", dem Bund also eine zusätzliche Verwaltungskompetenz eröffnet.[130]

Bereits dem Wortlaut des Art. 87 Abs. 3 GG ist zu entnehmen, dass dessen Anwendung voraussetzt, dass dem Bund für die betreffende Sachmaterie eine Gesetzgebungskompetenz zusteht. Darüber hinaus leitet die Rechtsprechung des BVerfG aus einem systematischen Vergleich mit Art. 87 Abs. 3 Satz 2 sowie Art. 87 Abs. 1 GG ab, dass es sich im Rahmen des Art. 87 Abs. 3 Satz 1 GG um eine Aufgabe handeln muss, die der Sache nach für das gesamte Bundesgebiet zentral durch ein Bundesoberbehörde ohne Mittel- und Unterbau und ohne Inanspruchnahme der Länder wahrgenommen werden können muss. Die Begründung einer Verwaltungszuständigkeit durch den Bund nach Art. 87 Abs. 3 Satz 1 GG ist demnach insoweit begrenzt, als die betreffende Sachaufgabe zur zentralen Erledigung geeignet sein muss und keines Verwaltungsunterbaus bedarf, der die Verwaltungszuständigkeit der Länder in erheblichem Umfang verdrängt. Für Aufgaben, die demgegenüber einen solchen Verwaltungsunterbau erfordern, ist nach Art. 87 Abs. 3 Satz 2 GG die Zustimmung des Bundesrates und der Mehrheit der Mitglieder des Bundestages notwendig.[131]

Zentrale Aufgaben zeichnen sich dabei insbesondere dadurch aus, dass sie eine bundesweit einheitliche Entscheidungspraxis erfordern und die Verwaltungstätigkeit einen großräumigen, überörtlichen Bezug aufweist, ohne maßgeblich von örtlichen Gegebenheiten geprägt zu sein.[132]

Für den Vollzug eines auf Art. 91c Abs. 5 GG gestützten Bundesgesetzes, das Regelungen zu einer Postfach- und Kommunikationsinfrastruktur trifft, sind die nach der Rechtsprechung des BVerfG im Rahmen des Art. 87 Abs. 3 Satz 1 GG zu erfüllenden Voraussetzungen – Eignung der Aufgabe zur zentralen Erledigung und kein Bedürfnis nach einem die Verwaltungszuständigkeit der Länder verdrängen Verwaltungsunterbau – nach unserem Kenntnisstand gegeben. Soweit ein solcher Unterbau erforderlich wäre, erscheint zudem auch eine Aufgabenübertragung auf bundeseigene Mittel- und Unterbehörden nach Art. 87 Abs. 3 Satz 2 GG bei entsprechender

[130] BVerfG, Beschluss vom 03.03.2004 – 1 BvF 3/92, Rn. 90.
[131] BVerfG, Beschluss vom 14.05.2007 – 1 BvR 2036/05, NVwZ 2007, 942 (944).
[132] Winkler, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 87, Rn. 50.

Begründung des dringenden Bedarfs und unter den dort vorgesehenen Zustimmungserfordernissen vorstellbar.

c) Folgerungen für die Machbarkeit von ZaPuK

Art. 91c Abs. 5 GG stellt grundsätzlich eine geeignete Rechtsgrundlage dar, um die Errichtung von ZaPuK ebenenübergreifend gesetzlich zu regeln. In Kombination mit Art. 87 Abs. 3 GG kann der Bund zudem den Vollzug der Regelungen soweit erforderlich durch Bundesgesetz an sich ziehen und auf eine bundeseigene Behörde übertragen.

Konkret bedeutet das insbesondere, dass durch Bundesgesetz beispielsweise einer nachgeordneten Behörde im Geschäftsbereich des BMDS die Aufgabe des Betriebs des zentralen Backends für Privatpersonen übertragen werden kann. Dies hätte zur Konsequenz, dass insoweit auch die Finanzierungsverantwortung für den Betrieb des Backends beim Bund läge.

Folgende Grenzen der Ermächtigungsgrundlage sind zu beachten:

- Art. 91c Abs. 5 GG erstreckt sich auf **Verwaltungsverfahren** im Sinne des § 9 VwVfG, nicht aber auf den Bereich der Justiz. Für die perspektivisch vorgesehene Einbindung des Elektronischen Rechtsverkehrs muss daher eine weitere Rechtsgrundlage herangezogen werden. Die Gesetzgebungskompetenzen des Bundes für die Gesetze zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) und zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 (BGBl. I S. 2208). ergeben sich ausweislich der Gesetzesbegründungen aus Art. 74 Abs. 1 Nr. 1 GG für das „gerichtliche Verfahren".

- Ein Anschluss der **Kommunen** an ZaPuK kann nach hier vertretener Auffassung auf Basis von Art. 91c Abs. 5 GG gesetzlich vorgegeben werden. Dies gilt jedoch nur insoweit, als den Kommunen dadurch keine erheblichen, einer Aufgabenübertragung vergleichbaren organisatorischen, personellen oder finanziellen Aufwände, zum Beispiel für Entwicklung oder Betrieb, entstehen sowie zugleich darauf geachtet wird, dass den Kommunen zur Anpassung von Lösungen an die örtlichen Gegebenheiten ein

hinreichender Gestaltungsspielraum verbleibt. Beides ist nach unserer Auffassung im Rahmen der Konzeption von ZaPuK grundsätzlich umsetzbar, da einerseits zentrale Organisationsbackends und Frontends bereitgestellt werden, von denen die Kommunen ohne großen Aufwand Gebrauch machen können, andererseits aber die Möglichkeit besteht, eigene Backends und Frontends zu gestalten. Für die konkrete Umsetzung sollte der Austausch mit den Kommunen gesucht werden.

- **Betrieb und Finanzierung**: Im Ausgangspunkt handelt es sich bei Art. 91c Abs. 5 GG um eine Gesetzgebungskompetenz. Für eine beim Bund zentralisierte Umsetzung, d.h. Entwicklung, Bereitstellung und Betrieb von ZaPuK sowie die damit nach dem Konnexitätsgrundsatz verbundene Finanzierung, sind daher weitergehende Rechtsgrundlagen in die Betrachtung miteinzubeziehen. Für einen Teilbereich von ZaPuK – den Betrieb des zentralen Backends für Privatpersonen – wird eine solche Verortung beim Bund angestrebt. Der Bund kann hierfür von Art. 87 Abs. 3 GG Gebrauch machen und den Vollzug insoweit an sich ziehen.

- Insoweit zeigen sich weitere Grenzen aus Art. 91c Abs. 5 GG als Ermächtigungsgrundlage: Eine Übertragung der Betriebsverantwortung für bestimmte IT-Komponenten auf die FITKO ist allein auf dieser Grundlage nicht möglich. Die gemeinsame Vollzugsverantwortung muss als Durchbrechung des Verbots der Mischverwaltung verfassungsrechtlich legitimiert sein, z.B. auf Basis von Art. 91c Abs. 1 GG (siehe dazu Abschnitte 2.2.3 und 2.3).

2.2.3. Zusammenwirken von Bund und Ländern nach Art. 91c Abs. 1 und 2 GG

Schließlich stellt sich die Frage, ob bzw. inwieweit das Vorhaben einer einheitlichen föderalen Postfach- und Kommunikationsinfrastruktur auf Grundlage von Art. 91c Abs. 1 und/oder Abs. 2 GG umsetzbar ist.

Art. 91c Abs. 1 GG kann als Generalklausel für das bund- und länderübergreifende – rechtliche und tatsächliche – Zusammenwirken im IT-Bereich verstanden werden. Art. 91c Abs. 2 GG bietet daneben eine gegenüber Art. 91c Abs. 1 GG enger gefasste Kooperationsmöglichkeit, die

inhaltlich auf die *Festlegung der für die Kommunikation zwischen den informationstechnischen Systemen erforderlichen Standards und Sicherheitsanforderungen* beschränkt ist.[133]

Im Einzelnen:

a) Reichweite der Generalklausel nach Art. 91c Abs. 1 GG

In Art. 91c Abs. 1 GG heißt es wörtlich:

> *Bund und Länder können bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken.*

Von der eröffneten Kooperationsmöglichkeit haben Bund und Länder durch den Abschluss des – im April 2010 in Kraft getretenen – sog. IT-Staatsvertrags[134] Gebrauch gemacht und den IT-Planungsrat eingerichtet, der gemäß § 1 Abs. 1 Satz 1 des IT-Staatsvertrags unter anderem die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik koordinieren soll (Nr. 1). Auf Basis seiner Neufassung im Jahr 2019 wurde mit Wirkung zum 01.01.2020 ferner die FITKO errichtet.[135]

Art. 91c Abs. 1 GG adressiert den Bund und die Länder. Die Kommunen werden dabei als Teil der Länder betrachtet, da diese aus staatsorganisationsrechtlicher und finanzverfassungsrechtlicher Sicht den Ländern zugeordnet werden.[136] Neben den Gebietskörperschaften sind auch

[133] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 18 und 21 f.

[134] Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern - Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag) vom 30. Oktober 2009 bis 30. November 2009 (BGBl. 2010 I S. 662), der durch Staatsvertrag vom 15. bis 21. März 2019 (BGBl. 2019 I S. 1126) und zuletzt durch Staatsvertrag vom 27. November bis 31. Dezember 2023 (BGBl. 2024 I Nr. 326) geändert worden ist.

[135] Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 11 f.

[136] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 19; Ruge, in: Schmidt-Bleibtreu, Grundgesetz, Kommentar, Hofmann/Hennecke (Hrsg.), 15. Auflage, Art. 91c, Rn. 18.

unter Bundes- oder Landesaufsicht stehende andere juristische Personen des öffentlichen Rechts – Körperschaften, Anstalten, Stiftungen – erfasst.[137]

Die Gesetzesbegründung deutet auf ein weites Normverständnis des verfassungsändernden Gesetzgebers hin, nach dem insbesondere die Möglichkeit, Vereinbarungen – Staatsverträge und Verwaltungsabkommen –[138] zur ebenübergreifenden Zusammenarbeit zu treffen und die hierfür erforderliche Gremienstruktur zu schaffen, in Art. 91c Abs. 1 GG angelegt ist. Dort heißt es konkret:

> *„Die Vorschrift ist angesichts des ständigen Fortschritts der Informationstechnik und ihrer wachsenden Bedeutung für die öffentliche Verwaltung weit gefasst. Bund und Länder sollen in die Lage versetzt werden, auf die mannigfaltigen Herausforderungen und Chancen der Informationstechnik, auch soweit sie heute noch unbekannt sind, angemessen und zeitnah zu reagieren. Die weite Fassung der Norm ermöglicht zudem die einheitliche Umsetzung der im IT-Bereich zunehmenden EU-Vorgaben.*
>
> *[…]*
>
> *Die Bund-Länder-Zusammenarbeit kann durch Vereinbarungen, in denen die Art und Weise der Zusammenarbeit näher ausgestaltet wird, geregelt werden. Für ihre Zusammenarbeit können Bund und Länder insbesondere die notwendige Gremienstruktur (IT-Planungsrat) schaffen und die hierfür erforderlichen Vereinbarungen treffen […].“*[139]

Der offen gehaltene Wortlaut des Art. 91c Abs. 1 GG eröffnet den Verwaltungsträgern also Spielraum für verschiedene Ausgestaltungen der Zusammenarbeit.[140] Ein tatsächliches

[137] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 19.
[138] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 17.
[139] Begründung zu Art. 91c GG, Gesetzentwurf der Fraktionen der CDU/CSU und SPD, BT-Drucksache 16/12410 vom 24.03.2009, S. 9.
[140] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 17.

Zusammenwirken kann sich etwa in der gemeinsamen Umsetzung konkreter Vorhaben – etwa beim Aufbau von Basisinfrastrukturen für E-Government – oder in informellen Abstimmungsprozessen ohne rechtlich verpflichtenden Charakter manifestieren.[141]

Die Kooperationsbefugnis erstreckt sich dabei auf sämtliche Abschnitte des Lebenszyklus informationstechnischer Systeme – die „Planung", „Errichtung" und den „Betrieb".[142]

Ein **Zusammenwirken in Bezug auf die Planung, Errichtung und den Betrieb einer IT-Infrastruktur für Postfach- und Kommunikationslösungen** ließe sich daher im Ausgangspunkt unter die Vorschrift subsumieren. Denkbar wäre insofern der Abschluss bzw. die Erweiterung eines Staatsvertrags zwischen Bund und Ländern gemäß Art. 91c Abs. 1 und 2 GG (zu Art. 91c Abs. 2 GG siehe sogleich), um in vergleichbarer Weise zum NOOTS-Staatsvertrag eine gemeinsame Steuerung und Finanzierung (siehe hierzu §§ 3 und 8 des NOOTS-Staatsvertrags) des Vorhabens zu regeln.

Eine Pflicht zur Kooperation begründet Art. 91c Abs. 1 GG nicht. Die Zusammenarbeit im IT-Bereich steht ausdrücklich im Ermessen von Bund und Ländern. Dies ergibt sich bereits aus der gewählten Formulierung der Bestimmung („können"). Der Grundsatz der Bundestreue gebietet aber, dass einzelne Länder, die selbst nicht zur Zusammenarbeit bereit sind, eine Kooperation zwischen dem Bund und kooperationswilligen Ländern nicht verhindern dürfen.[143]

In Bezug auf ZaPuK spricht im Grundsatz viel dafür, dass eine kooperative Lösung nach Art. 91c Abs. 1 GG vereinbart werden kann, da Bund und Länder im Rahmen der 50. Sitzung des IT-Planungsrats bereits ihre Bereitschaft signalisiert haben, verbindlich die Anbindung und

[141] Ruge, in: Schmidt-Bleibtreu, Grundgesetz, Kommentar, Hofmann/Hennecke (Hrsg.), 15. Auflage, Art. 91c, Rn. 19.
[142] Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Band 3, Art. 83-146, 8. Auflage 2024, Art. 91c, Rn. 13.
[143] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 20; Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 11; Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 10.

Flächendeckung der Basiskomponenten einschließlich ZaPuK sicherzustellen und sich zur Nutzung zu verpflichten.[144]

b) Ergänzung durch Art. 91c Abs. 2 GG

Ergänzt wird die Generalklausel des Art. 91c Abs. 1 GG durch die enger gefasste Kooperationsmöglichkeit von Bund und Ländern nach Art. 91c Abs. 2 GG. Die Vorschrift konkretisiert die ebenenübergreifende Zusammenarbeit sowohl in formeller Hinsicht durch die Bindung an *Vereinbarungen* als auch in inhaltlicher Hinsicht:

> *[1]Bund und Länder können auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen. [2]Vereinbarungen über die Grundlagen der Zusammenarbeit nach Satz 1 können für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben vorsehen, dass nähere Regelungen bei Zustimmung einer in der Vereinbarung zu bestimmenden qualifizierten Mehrheit für Bund und Länder in Kraft treten. [3]Sie bedürfen der Zustimmung des Bundestages und der Volksvertretungen der beteiligten Länder; das Recht zur Kündigung dieser Vereinbarungen kann nicht ausgeschlossen werden. [4]Die Vereinbarungen regeln auch die Kostentragung.*
>
> (Hervorhebung hier hinzugefügt)

Aus dem Wortlaut von Art. 91c Abs. 2 Satz 1 GG geht hervor, dass sich sein Anwendungsbereich auf *notwendige Standards und Sicherheitsanforderungen* beschränkt. Eine nähere Erläuterung der Begriffe ergibt sich aus Art. 91c Abs. 2 GG dabei nicht. Der Begriff „Standards" kann nach der Kommentarliteratur etwa das Datenformat, die Datenübertragung, die Fonttechnologie, die Funkkommunikation, Grafiken, Maßeinheiten oder Messgrößen betreffen.[145] Der Begriff kann dabei sowohl *technische Standards* als auch organisations- und verfahrensbezogene Vorgaben umfassen, soweit diese die Kommunikation zwischen IT-Systemen betreffen

[144] Vgl. IT-Planungsrat, Beschluss 2026/18 vom 17. Juni 2026, Ziffer 5.
[145] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 24.

(*prozessuale Standards*). Als Standards können dabei auch konkrete Verfahren und Produkte sowie allgemeine Zielvorgaben oder Qualitätsniveaus bestimmt werden. Unter dem Begriff „Sicherheitsanforderungen" sind solche Standards zu verstehen, die die Informationssicherheit betreffen (siehe z.B. die IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik).[146] Aus der Formulierung „*zwischen*" in Art. 91c Abs. 2 Satz 1 GG geht hervor, dass die Bestimmung maßgeblich durch den Gedanken der Interoperabilität zwischen den unterschiedlichen föderalen Ebenen getragen ist.[147] Ferner müssen die Standards und Sicherheitsanforderungen *notwendig* sein. Danach ist bei ihrer Festlegung im Sinne einer Erforderlichkeitsprüfung zu untersuchen, ob gleich geeignete und ebenso leistungsfähige Alternativen zur Herstellung der Interoperabilität existieren. Dabei können auch wirtschaftliche Erwägungen berücksichtigt werden.[148]

Eine föderal einheitliche Postfach- und Kommunikationslösung betrifft mitunter die Herstellung interoperabler Kommunikationsstrukturen zwischen den informationstechnischen Systemen von Bund und Ländern und fällt damit gegebenenfalls in Teilen in den durch Art. 91c Abs. 2 Satz 1 GG eröffneten Regelungsbereich. Eine Besonderheit bei Anwendung des Art. 91c Abs. 2 GG besteht nach seinem Satz 4 darin, dass Vereinbarungen im Sinne des Art. 91c Abs. 2 Satz 1 GG auch Bestimmungen zur Kostentragung enthalten müssen. Ein konkreter Verteilungsschlüssel ist dabei nicht vorgegeben, sodass die Ausgestaltung der Kostenaufteilung grundsätzlich der freien Vereinbarung der Beteiligten überlassen bleibt.[149]

[146] Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Band 3, Art. 83-146, 8. Auflage 2024, Art. 91c, Rn. 24.
[147] Ruge, in: Schmidt-Bleibtreu, Grundgesetz, Kommentar, Hofmann/Hennecke (Hrsg.), 15. Auflage, Art. 91c, Rn. 23.
[148] Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, Kommentar, Band 3, Art. 83-146, 8. Auflage 2024, Art. 91c, Rn. 24.
[149] Heun/Thiele, in: Dreier, Grundgesetz Kommentar, 3. Auflage, Band III, Art. 83-146, Art. 91c GG, Rn. 19; Suerbaum, in: BeckOK Grundgesetz, Epping/Hillgruber, 62. Edition, Stand: 15.06.2025, Art. 91c, Rn. 17.

c) Zulässigkeit und Grenzen für eine zentrale Bereitstellung und Finanzierung der IT-Infrastruktur durch den Bund

Fraglich ist, ob Art. 91c Abs. 1 und 2 GG als weitreichende Kooperationsvorschriften dem Bund jenseits eines gleichberechtigten Zusammenwirkens im engeren Sinne auch die Befugnis eröffnen, IT-Infrastrukturen zentral bereitzustellen und zu finanzieren. Im Einzelnen:

Die Norm ist darauf ausgerichtet, die Kooperation von Bund und Ländern verfassungsrechtlich zu legitimieren und dadurch rechtliche Unsicherheiten zu beseitigen, die sich aus dem grundsätzlichen Verbot der Mischverwaltung für den bund- und länderübergreifenden Aufbau und Betrieb informationstechnischer Systeme folgen. Art. 91c Abs. 1 GG kann dabei als lex specialis zum u.a. in Art. 104a Abs. 1 GG verankerten Trennungs- und Konnexitätsprinzip verstanden werden, nach dem die jeweiligen Hoheitsträger die ihnen zugewiesenen Aufgaben gesondert finanzieren. Eine generelle Aufgabe des verfassungsrechtlichen Kompetenzgefüges im Bereich der Digitalisierung dürfte durch die Norm dabei jedoch nicht begründet werden. Insbesondere ergibt sich aus Art. 91c GG weder eine allgemeine Zuständigkeit des Bundes für Digitalisierungsaufgaben, die es dem Bund erlauben würde, sämtliche Regelungsbereiche im Umfeld der digitalen Transformation an sich zu ziehen, noch eine umfassende Finanzierungsbefugnis.[150]

Wie Aufgaben- und Finanzierungsverantwortung für die informationstechnischen Systeme im Rahmen von Art. 91c Abs. 1 GG im Einzelnen zu verteilen sind, ist verfassungsrechtlich nicht abschließend geklärt. Da sich der Norm hierzu keine konkreten Vorgaben entnehmen lassen, bildet zunächst weiterhin die grundgesetzliche Verteilung von Verwaltungs- und Finanzierungskompetenzen nach den Prinzipien der Eigenverantwortung und Konnexität den Ausgangspunkt für das in Art. 91c Abs. 1 GG vorgesehene Zusammenwirken.

Die Annahme einer Bündelungsmöglichkeit einer umfassenden Steuerungs- und Finanzverantwortung ausschließlich bei einem einzigen Rechtsträger – dem Bund – stößt demgegenüber auf deutliche Kritik: Eine solche Zentralisierung könne dem Begriff des „Zusammenwirkens“ in Art. 91c Abs. 1 GG nicht mehr gerecht werden. Denn zwingende Voraussetzung sei insofern

[150] M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 20.

eine **Kooperation** zwischen unterschiedlichen Hoheitsträgern. Die kompetenzielle Tragweite der Art. 91c Abs. 1 bis 3 GG sei deutlich begrenzter als jene der Art. 91c Abs. 4 und 5 GG, die dem Bund ausdrückliche Gesetzgebungsbefugnisse zuordneten. Der Wortlaut des Art. 91c Abs. 1 GG trage insofern auch keine Auslegung, die darüber hinausgehende Vereinbarungen über eine vollständige Zentralisierung der IT-Infrastruktur zuließe und den kooperativen Gehalt der Vorschrift unterliefe.[151]

Nicht ausgeschlossen erscheint aber, dass unter die offene Kooperationsmöglichkeit des Art. 91c Abs. 1 GG auch eine **Leistung einer föderalen Ebene für eine andere** gefasst werden kann, sofern diese freiwillig erfolgt. Ein solches Zusammenwirken sei verfassungsrechtlich bereits in der offen gestalteten Struktur der Vorschrift angelegt, da diese keinen konkreten Formenzwang für die Art und Weise der Kooperation im IT-Bereich beinhalte. Insofern könne auf Grundlage von Art. 91c Abs. 1 GG als freiwilliges Angebot auch eine zentrale Bereitstellung digitaler Infrastrukturen erfolgen. Dabei wird jedoch auch darauf hingewiesen, dass die beschriebene freiwillige Konstruktion im Hinblick auf das Konnexitätsprinzip aus Art. 104a Abs. 1 GG finanzverfassungsrechtlich nicht unproblematisch sei.[152]

Nach der hier vertretenen Auffassung sind vor diesem Hintergrund verschiedene Ausgestaltungen von Vollzug und Finanzierung im Kontext der Gestaltung der informationstechnischen Systeme denkbar. Die Grenzen eines „Zusammenwirkens" dürfen jedoch nicht verlassen werden. Eine zentrale Umsetzung und Finanzierung von ZaPuK allein auf Basis von Art. 91c Abs. 1 und 2 GG wäre jedenfalls mit erheblichen verfassungsrechtlichen Risiken verbunden und ist nicht zu empfehlen.

Allerdings könnte eine freiwillige Zurverfügungstellung einer zentral durch den Bund errichteten und finanzierten IT-Infrastruktur grundsätzlich in eine Vereinbarung nach Abs. 1 einbezogen werden, wenn sich die Bereitstellung und Finanzierung durch den Bund bereits im Rahmen der ihm nach Art. 86 ff. GG zugewiesenen Verwaltungskompetenz und der damit

[151] Martini/Botta: Government-as-a-Platform - Vorschlag einer Änderung des Grundgesetzes zur Staatsmodernisierung, NJW 2025, 1464 (1467), Rn. 29-31.
[152] Roth-Isigkeit, Verfassungsrechtliche Möglichkeiten der Aufgabenbündelung im Föderalstaat, Rechtsgutachten im Auftrag des Nationalen Normenkontrollrats (NKR), S. 50 f.

konnexitätsrechtlich einhergehenden Finanzierungsbefugnis bewegt (vgl. dazu bereits 2.1.1). Stellt der Bund die für seine eigenen Verwaltungseinrichtungen entwickelten IT-Komponenten den Ländern anschließend im Wege des Zusammenwirkens nach Art. 91c Abs. 1 GG zur Nutzung zur Verfügung, folgt daraus grundsätzlich weder die oben angesprochene generelle Aufgabe des verfassungsrechtlichen Kompetenz- und Finanzierungsgefüges, noch ist darin eine unzulässige Ausdehnung des Wortlauts von Art. 91c Abs. 1 GG zu erkennen. Zu berücksichtigen ist aber auch insoweit das in Art. 91c Abs. 1 GG enthaltene Element der Kooperation und Arbeitsteilung; eine einseitige Verortung aller Verantwortlichkeiten und Lasten auf Seiten des Bundes gibt die Rechtsgrundlage nicht her. Ein kooperatives Element könnte aufgrund der zuvor beschriebenen offenen Gestaltung der Norm bereits in einer weniger intensiv ausgestaltenden Abstimmung zwischen Bund und Ländern liegen – etwa in Form einer informellen Absprache hinsichtlich einer Simultangesetzgebung bzw. eines Simultanverwaltungsvollzugs zur Umsetzung der Anschlussbedingungen für die Nutzung der IT-Infrastruktur. Je nach Aufwand auf Bundesseite könnten aber auch weitere Beiträge der Länder erforderlich werden.

Zu berücksichtigen ist zudem, dass mit dem IT-Staatsvertrag und seiner institutionellen Umsetzung in Gestalt von IT-Planungsrat und FITKO bereits eine Kooperation gemäß Art. 91c Abs. 1 und 2 GG vorhanden ist. Diese könnte gegebenenfalls auch für die Zwecke von ZaPuK genutzt und um weitere erforderliche Kooperationselemente und Regelungen erweitert werden.

d) Folgerungen für die Machbarkeit von ZaPuK

Wie zuvor unter a) festgestellt, kommt als Rechtsgrundlage für die Umsetzung der Postfach- und Kommunikationsinfrastruktur der Abschluss eines Staatsvertrags zwischen Bund und Ländern gemäß Art. 91c Abs. 1 und 2 GG in Betracht, der analog zum NOOTS-Staatsvertrag Bestimmungen über eine gemeinsame Steuerung und Finanzierung des Vorhabens durch Bund und Länder beinhaltet:

- Ein Vorteil dieser kooperativen Lösung liegt in der größeren Flexibilität hinsichtlich der Ausgabenzuordnung. Im Rahmen des Art. 91c Abs. 1 GG müssen die Kosten für Planung, Errichtung und der Betrieb des gemeinsam benötigten informationstechnischen Systems nicht zwingend entsprechend der tatsächlichen Nutzung kleinteilig für

einzelne Bundes- und Landesverwaltungsaufgaben aufgeteilt werden, sondern ihre Verteilung kann zwischen den beteiligten Hoheitsträgern auch anhand eines abstrakten, sachgerechten Finanzierungsschlüssels vereinbart werden.

- Darüber hinaus erlaubt die Rechtsgrundlage ein Zusammenwirken auch in Gestalt einer gemeinsamen Einrichtung. Ausgehend von dem IT-Staatsvertrag oder ergänzenden/vergleichbaren staatsvertraglichen Regelungen können daher auf diesem Wege auch Aufgaben und Verwaltungszuständigkeiten (z.B. für den Betrieb des zentralen Backends für Organisationen) auf die FITKO übertragen werden.

- Sollen jedoch *allein auf Basis von Art. 91c Abs. 1 und 2 GG* dem Bund zentrale Befugnisse bzw. Pflichten zur Errichtung, zum Betrieb und zur Finanzierung der Postfach- und Kommunikationsinfrastruktur eingeräumt werden, wäre dies mit erheblichen verfassungsrechtlichen Risiken verbunden. Für solche Elemente der Postfach- und Kommunikationsinfrastruktur, die zentral beim Bund liegen sollen, sollte daher auf andere verfassungsrechtliche Grundlagen zurückgegriffen werden (s. näher dazu Abschnitt 2.3).

- Ein **Staatsvertrag** erfüllt in diesem Fall eine weitere wichtige Funktion: Führen verschiedene Rechtsgrundlagen zu kompetenziellen Überschneidungen oder Unsicherheiten, können und sollten diese zur Vermeidung von Mischverwaltung und Mischfinanzierung durch Vereinbarung konkretisiert und klargestellt werden.[153] Finanzierungsanteile werden dabei nicht frei festgelegt, sondern orientieren sich an den jeweils zugrunde gelegten und in die Kooperation einfließenden Verwaltungszuständigkeiten (vgl. auch Abschnitt 2.3).

2.2.4. Zusammenwirken von Bund und Ländern im Bereich der Finanzverwaltung

Neben den bereits angesprochenen allgemeinen verfassungsrechtlichen Rechtsgrundlagen sind in ein solches Modell auch jene Verwaltungs- und Gesetzgebungskompetenzen einzubeziehen, die das Grundgesetz speziell für den Verwaltungsvollzug im Bereich der

[153] Vgl. Siekmann, in: Sachs, Grundgesetz, 10. Auflage 2024, Art. 104a, Rn. 18.

Finanzverwaltung vorhält. Soll die Kommunikation mit den Steuerbehörden in die geplante einheitliche Postfach- und Kommunikationsinfrastruktur integriert werden, muss auch für diese Einbindung eine verfassungsrechtliche Grundlage zur Verfügung stehen.

Eine solche Rechtsgrundlage könnte insbesondere Art. 108 Abs. 4 Satz 1 GG sein. Die dort niedergelegte Möglichkeit der Kooperation geht dem Art. 91c GG als speziellere Regelung vor.[154] Allerdings sind nur punktuelle Durchbrechungen der Kompetenzordnung zulässig. Die in Art. 108 Abs. 4 Satz 1 GG eröffnete Regelungsbefugnis setzt auf Tatbestandsebene voraus, dass der Vollzug der Steuergesetze erheblich verbessert oder erleichtert wird. Dem Gesetzgeber steht diesbezüglich ein Beurteilungsspielraum zu. Bereits das Ziel einer (beträchtlichen) Kosteneinsparung kann die Annahme einer entsprechenden Verbesserung oder Erleichterung des Gesetzesvollzugs rechtfertigen.[155]

Einfachgesetzliche Ausformung hat die Kooperationsmöglichkeit bereits in §§ 20, 21a FVG und im Gesetz über die Koordinierung der Entwicklung und des Einsatzes neuer Software der Steuerverwaltung (KONSENS-G) erhalten.[156] Ausweislich der Gesetzesbegründung ergänzt das KONSENS-G die Regelung des § 20 Abs. 2 FVG, der das Zusammenwirken der obersten Finanzbehörden des Bundes und der Länder beim Vollzug der von den Landesfinanzbehörden im Auftrag des Bundes verwalteten Steuern regelt und der ein gegenüber der ursprünglichen Regelung tatbestandlich erweitertes IT-fachliches Weisungsrecht des Bundes beinhaltet. Ferner sollten die Regelungen des im Jahr 2007 in Kraft getretenen Verwaltungsabkommens zur Regelung der Zusammenarbeit im Vorhaben KONSENS (Koordinierte neue Software-Entwicklung der Steuerverwaltung), soweit sie den Bereich der Bundesauftragsverwaltung betreffen, mit dem KONSENS-G in eine gesetzliche Regelung überführt werden. Das Zusammenwirken von

[154] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 10; Th. Wischmeyer, in: v. Mangoldt/Klein/Starck, GG, Grungesetz, Kommentar, Band 3, Art. 83-146, 7. Auflage, Art. 91c, Rn. 12.

[155] Schenke, in: Grundgesetz für jede(n), Der Grundgesetzkommentar von Prof. Dr. Helge Sodan, Art. 108 Rn. 11, abrufbar unter https://www.grundgesetz-fuer-jeden.de/artikel-108.html), zuletzt abgerufen am 20.01.2026.

[156] Gröpl, in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, August 2018, Lfg. 84, Art. 91c GG, Rn. 10 und 77.

Bund und Ländern beim Einsatz automatischer Einrichtungen für die Festsetzung und Erhebung der Steuern erfolgte zuvor auf der Grundlage des Verwaltungsabkommens KONSENS.[157]

Diese derzeitige Ausgestaltung der Zusammenarbeit von Bund und Ländern im Rahmen von KONSENS (Verwaltungsabkommen und KONSENS-G) ist allerdings nicht als verfassungsrechtliches Hindernis zu bewerten, sondern lediglich als Ausdruck einer aktuellen praktischen föderalen Kooperation. Für eine weitergehende Nutzung des Art. 108 Abs. 4 GG, um auf dieser Grundlage die Nutzung von ZaPuK im Bereich der Finanzverwaltung zu etablieren, muss im Einzelnen aufgezeigt werden, dass ZaPuK zu einer erheblichen Verbesserung oder Erleichterung des Vollzugs der Steuergesetze beiträgt.

Die Regelung einer föderal einheitlichen Postfach- und Kommunikationsstruktur erscheint demnach durch Bundesgesetz mit Zustimmung des Bundesrates auf der Grundlage von Art. 108 Abs. 4 Satz 1 und 3 GG und – soweit der Aufbau und das Verfahren betroffen sind – auf Basis von Art. 108 Abs. 1 Satz 2, Abs. 2 Satz 2, Abs. 3 Satz 1 und 2 und Abs. 5 GG möglich.

Folgerungen für ZaPuK

Eine Erstreckung von ZaPuK auch auf die Steuerverwaltung kann mittels Bundesgesetzes mit Zustimmung des Bundesrates erfolgen. Die Regelung setzt dann implizit voraus, dass Errichtung und Betrieb von ZaPuk bereits auf anderweitiger Rechtsgrundlage geregelt sind und realisiert werden. Zu empfehlen ist aber, die Finanzministerien von Bund und Ländern frühzeitig bei der Ausgestaltung von ZaPuK als Entscheidungsträger mitzuberücksichtigen, um die notwendige Kompatibilität der Architektur mit den besonderen Anforderungen der Steuerverwaltung sicherzustellen.

[157] Begründung zum KONSENS-G, Beschlussempfehlung und Bericht des Haushaltsausschusses (8. Ausschuss), BT-Drucksache 18/12589 vom 31.05.2017, S. 132.

2.3. Folgerungen für ZaPuK: Herleitung der rechtlichen Machbarkeit des Gesamtvorhabens durch Zusammenführung der verschiedenen Gesetzgebungs- und Verwaltungskompetenzen

Die Umsetzung von ZaPuK ist – das ist in den einzelnen vorstehenden Abschnitten deutlich geworden – nicht auf Grundlage einer einzigen verfassungsrechtlichen Grundlage in zufriedenstellender Weise realisierbar. Eine Realisierung der derzeit vorgesehenen Zielarchitektur kann jedoch auf der Grundlage einer Kombination der verschiedenen verfassungsrechtlichen Rechtsgrundlagen erfolgen:

- Der Bund kann für seine bundeseigene Verwaltung gemäß Art. 86 GG in Verbindung mit Art. 104a Abs. 1 GG die erforderliche Postfach- und Kommunikationsinfrastruktur entwickeln, bereitstellen und finanzieren. Dies ermöglichte die im Architekturkonzept vorgesehene zentrale Entwicklung der Software-Komponenten gebündelt beim Bund (bzw. durch dessen Dienstleister).

- Eine weitere Gesetzgebungszuständigkeit des Bundes kann aus Art. 91c Abs. 5 GG abgeleitet werden. Diese deckt alle Regelungen im Zusammenhang mit dem durch ZaPuK eröffneten Zugang für private Personen und Organisationen zu Verfahren und Leistungen der Verwaltung ab, einschließlich aller erforderlichen Gesetzesanpassungen zur Etablierung der Postfachstruktur sowie zur Anschlussverpflichtung von Ländern und Gemeinden. In Verbindung mit Art. 87 Abs. 3 GG erlaubt die Gesetzgebungskompetenz des Art. 91c Abs. 5 GG dem Bund zudem, die Verwaltung des zentralen Backends für Privatpersonen wie im Architekturkonzept vorgesehen an sich zu ziehen und auf eine bundeseigene Verwaltungseinheit – zum Beispiel eine nachgeordnete Behörde im Geschäftsbereich des BMDS – zu übertragen. Sollte dies gewünscht sein, könnte eine solche Aufgabenübertragung auch auf weitere Verwaltungszuständigkeiten wie beispielsweise den Betrieb des zentralen Backends für private Organisationen erweitert werden. Der damit begründeten Vollzugszuständigkeit folgt dann jeweils auch die Finanzierungszuständigkeit für den Betrieb des zentralen Postfach-Backends.

- Schließlich empfehlen wir auf Basis von Art. 91c Abs. 1 und 2 GG den Abschluss eines Staatsvertrags zur übergreifenden Regelung des Zusammenwirkens in Bezug auf ZaPuK. Ein solcher Staatsvertrag würde zugleich eine Handhabung für verbindliche Vorgaben über die Ablösung bestehender Postfach- und Kommunikationslösungen eröffnen. Im Rahmen dieser Kooperation halten wir es auch für zulässig, dass der Bund seine zentral entwickelten Backend-Komponenten den Behörden auf Länder- und Gemeindeebene zur Verfügung stellt. Bestandteil einer solchen Regelung müsste insbesondere auch die Zuteilung der Zuständigkeiten für den Betrieb der weiteren zentralen Backends sein. Als Gegenstand der Kooperation nach Art. 91c Abs. 1 GG können diese wie im Architekturkonzept vorgesehen über den IT-Planungsrat an die FITKO delegiert werden. Zu beachten ist, dass für die an die FITKO delegierten Aspekte der Infrastruktur jedoch keine alleinige Finanzierung durch den Bund in Betracht kommt (siehe D.I.2.2.3.c)). Ein Staatsvertrag eröffnet zwar zusätzlichen Gestaltungsspielraum für die Finanzierungsbeiträge der Beteiligten. Es ist aber davon auszugehen, dass sich die Finanzierungsverantwortung im Ausgangspunkt nach der Vollzugszuständigkeit richtet. Bedienen sich die Beteiligten für den Betrieb der FITKO, so liegt es nahe, auch bezüglich der Finanzierung der Tätigkeit den bei der FITKO etablierten Finanzierungsmechanismen zu folgen und den modifizierten Königsteiner Schlüssel anzuwenden.

- Es muss nicht zwingend ein neuer „ZaPuK-Staatsvertrag" geschlossen werden, um die notwendigen Regelungen zur Zusammenführung, Konkretisierung und Klarstellung der verschiedenen Verwaltungs- und Finanzierungsanteile zu treffen. Denkbar wäre ebenso eine übergreifende Vereinbarung in Gestalt eines „D-Stack-Staatsvertrags", ggf. anknüpfend an den NOOTS-Staatsvertrag, oder auch eine Ergänzung des bestehenden IT-Staatsvertrag um Regelungen zur Kooperation in Sachen ZaPuK.

3. Grundgesetzänderung zur Umsetzung von ZaPuK

Nach dem Ergebnis der vorangegangenen Prüfung ist die Machbarkeit einer föderal einheitlichen Postfach- und Kommunikationsstruktur bereits auf Basis des verfassungsrechtlichen Ist-Zustands gegeben. Eine Änderung des GG ist zur Umsetzung des hier gegenständlichen

Vorhabens daher nicht zwingend erforderlich. Nichtsdestotrotz erscheint eine Grundgesetzänderung im Interesse einer größeren Rechtssicherheit und -klarheit wünschenswert.

Eine solche Änderung ist bereits im Rahmen der am 4. Dezember 2025 von der Ministerpräsidentenkonferenz beschlossenen föderalen Modernisierungsagenda als Maßnahme 201 vorgesehen: Danach streben Bund und Länder eine zeitnahe Änderung von Artikel 91c GG an, damit der Bund digitale Verfahren und Standards regeln und IT-Systeme errichten, betreiben und für die Mitnutzung durch die Landesebene zur Verfügung stellen kann.[158] Auf eine solche Norm könnten auch in Bezug auf ZaPuK die zentrale Entwicklung, Bereitstellung, der Betrieb und die Mitnutzung gestützt werden. Der Vorteil bestünde insbesondere darin, dass das vorstehend beschriebene Stückwerk an Zuständigkeiten vermieden wird und insbesondere auch mit Blick auf künftige Anpassungen und Weiterentwicklungen sowie die Sicherstellung des Betriebs eine klare und einheitliche Verantwortung gegeben wäre.

II. Verwaltungsverfahrensrechtliche Rahmenbedingungen für die Umsetzbarkeit – Relevante Vorgaben zur digitalen Kommunikation auf Bundessebene

Im Folgenden werden die derzeit auf Bundesebene geltenden zentralen verwaltungsverfahrensrechtlichen Vorgaben zur digitalen Kommunikation dargestellt, sofern und soweit sie für das in Rede stehende Vorhaben von Bedeutung sind.

Dabei soll insbesondere auf die Regelungen

- des allgemeinen Verwaltungsverfahrensrechts - insbesondere § 3a VwVfG („Elektronische Kommunikation“), § 41 VwVfG („Bekanntgabe des Verwaltungsaktes“) -,
- des OZG - insbesondere § 9 OZG („Bekanntgabe des Verwaltungsaktes“) - sowie
- die für den Bereich der Steuerverwaltungsverfahren - insbesondere § 87a AO („Elektronische Kommunikation“), § 122 AO („Bekanntgabe des Verwaltungsakts“) und § 122a

[158] Besprechung des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder am 4. Dezember 2025, Beschluss, Die Föderale Modernisierungsagenda, Maßnahme 201, abrufbar unter https://bmds.bund.de/themen/staatsmodernisierung/modernisierungsagenda-foederal, zuletzt abgerufen am 31.08.2026.

AO („Bekanntgabe von Verwaltungsakten durch Bereitstellung zum Datenabruf") - und

- die für den Bereich der Sozialverwaltungsverfahren bestehenden Sonderregelungen für die digitale Kommunikation - § 36a des ersten Sozialgesetzbuchs (SGB I) („Elektronische Kommunikation") und § 37 des zehnten Sozialgesetzbuchs (SGB X) („Bekanntgabe des Verwaltungsaktes") - eingegangen werden.

Die Architektur von ZaPuK ist nach geltender Rechtslage grundsätzlich an diesen Vorgaben auszurichten, soweit sie die elektronische Kommunikation in den genannten Bereichen abbilden können soll. Dabei ist jedoch zu berücksichtigen, dass sich die verwaltungsverfahrensrechtlichen Rahmenbedingungen derzeit im Wandel befinden:

- Zum einen wurde durch das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 3. Juli 2026[159] angeordnet, dass das De-Mail-Gesetz (De-Mail-G) mit Ablauf des 31. Dezember 2026 außer Kraft tritt, und dies in den Verfahrensordnungen bereits entsprechend berücksichtigt.

- Zum anderen sieht dasselbe Gesetz Änderungen der Bestimmungen über die elektronische Kommunikation (insbesondere § 3a VwVfG) vor, die erst innerhalb des nächsten Jahres in Kraft treten sollen.

- Ferner ist vorgesehen, dass der Bund im Rahmen der Maßnahme 207 der von der Ministerpräsidentenkonferenz beschlossenen föderalen Modernisierungsagenda die Vorschriften über die digitale Bekanntgabe und Zustellung von Verwaltungsakten im Hinblick auf föderale Postfachlösungen harmonisiert.[160]

[159] Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 03.07.2006, BGBl. 2026 I Nr. 199.

[160] Besprechung des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder am 4. Dezember 2025, Beschluss, Die Föderale Modernisierungsagenda, Maßnahme 207, abrufbar unter https://bmds.bund.de/themen/staatsmodernisierung/modernisierungsagenda-foederal, zuletzt abgerufen am 31.08.2026.

Diese Änderungen können sich auf die rechtliche Bewertung des Vorhabens auswirken und sind daher bei der Konzeption im Blick zu behalten.

Eine Darstellung der einzelnen, für die Umsetzung von ZaPuK ggf. relevanten Verfahrensvorschriften der Länder erscheint in Ansehung der aktuellen Harmonisierungsbestrebungen an dieser Stelle nicht geboten, da davon auszugehen ist, dass im Wege der Simultangesetzgebung auch auf landesrechtlicher Ebene Anpassungen erfolgen werden.

1. Eröffnung des Zugangs für elektronische Kommunikation durch Empfänger

Kurzzusammenfassung: Für die elektronische Kommunikation gilt der Freiwilligkeitsgrundsatz. Die elektronische Übermittlung setzt voraus, dass der Empfänger hierfür einen Zugang eröffnet hat (vgl. § 3a Abs. 1 VwVfG, § 36a Abs. 1 SGB I, § 87a Abs. 1 Satz 1 AO, § 5 Abs. 5 Satz 1 Verwaltungszustellungsgesetz (VwZG)). Die Zugangseröffnung muss sich dabei auf den jeweiligen elektronischen Kommunikationskanal beziehen und ausdrücklich oder zumindest konkludent erfolgen.

An eine konkludente Zugangseröffnung durch Privatpersonen werden bislang strenge Anforderungen gestellt. Das bloße Vorhalten eines Postfachs genügt nicht. Die Gesetzesmaterialien zu dem Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern deuten jedoch auf eine Abkehr von dieser Verkehrsauffassung hin. Danach könne die Zugangseröffnung bei Privatpersonen sehr niederschwellig erfolgen, etwa durch die Angabe der E-Mail-Adresse in einem Dokument. Für Unternehmen und im beruflichen Kontext auftretende natürliche Personen gelten bereits nach bisheriger Verkehrsauffassung weniger strenge Maßstäbe für die Annahme einer konkludenten Zugangseröffnung.

Danach ist davon auszugehen, dass bereits die Angabe einer Rückantwortadresse im Rahmen der Antragstellung als konkludente Zugangseröffnung genügt. Für einen proaktiven digitalen Schriftverkehr außerhalb eines konkreten Antragsverfahrens mit Organisationen erscheint es darüber hinaus vertretbar, auch die Registrierung im Self-Service-Portal (vgl. ADR-0008, ADR-1103 und ADR-1104) in Verbindung mit der Hinterlegung der Postfachadresse eines

Funktionspostfachs im Adressregister (ADR 1111) als konkludente Zugangseröffnung anzusehen (vgl. Abschnitt 5.1, 5.4.6 und 5.5.1.1 des Konzepts).

Eine proaktive elektronische Kommunikation der Verwaltung mit Privatpersonen – die Übermittlung oder Bekanntgabe ohne vorherige Mitwirkung der betroffenen Person – ist nach geltendem Recht dagegen regelmäßig unzulässig. Für ZaPuK tritt eine technische Hürde hinzu: Die pseudonyme, bereichsspezifische Adresse einer Privatperson entsteht erst nach einer Authentisierung, sodass der Behörde ohne vorangegangene Interaktion keine Adresse vorliegt (ADR-1105, ADR-1111; Abschnitt 5.5.2 und 5.5.2.3 des Konzepts).

Das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern verschiebt zwar den Ausgangspunkt – der zum 1. Juli 2027 in Kraft tretende neue § 3a Abs. 1 VwVfG bestimmt, dass die Kommunikation zwischen Behörden und Beteiligten elektronisch erfolgen *soll* –, hält an der vorherigen Zugangseröffnung durch die Privatperson aber ausdrücklich fest. Nach der Gesetzesbegründung bleibt eine elektronische Zugangseröffnung seitens der Privatperson weiterhin erforderlich, weil keine allgemeine Pflicht besteht, dem Staat eine digitale Adresse mitzuteilen. Die Reform bekräftigt damit das Freiwilligkeitsprinzip, statt es aufzuheben; die technische Hürde besteht ohnehin fort. Eine allgemeine proaktive Zustellung setzt deshalb eine ausdrückliche spezialgesetzliche Grundlage mit Fiktionswirkung und eine tragfähige Lösung für die Adressverfügbarkeit voraus.

1.1. Ausgangspunkt: Freiwilligkeitsgrundsatz und Zugangseröffnung

Nach § 3a Abs. 1 VwVfG ist die Übermittlung elektronischer Dokumente nur zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Die Parallelvorschriften des § 36a Abs. 1 SGB I und des § 87a Abs. 1 Satz 1 AO sowie – für die förmliche Zustellung – § 5 Abs. 5 Satz 1 VwZG sind wortgleich.

Für die elektronische Kommunikation gilt der Freiwilligkeitsgrundsatz. Das bedeutet, dass der Einsatz elektronischer Kommunikationsformen grundsätzlich nur dort und nur soweit möglich ist, wo sowohl die Behörde als auch der Verwaltungsadressat (Bürgerinnen und Bürger bzw. Unternehmen) in objektiver Hinsicht die hierfür erforderlichen Voraussetzungen geschaffen

(Zugang) und subjektiv den jeweiligen Kommunikationsweg ausdrücklich oder zumindest konkludent für den Rechtsverkehr geöffnet (Widmung) haben.[161] Die Widmung ist unter Berücksichtigung der Verkehrsanschauung zu ermitteln.[162] Verwendet ein Kommunikationspartner einen zwar faktisch verfügbaren, jedoch nicht für die elektronische Kommunikation gewidmeten Zugang, geht das Dokument auch dann nicht zu, wenn es tatsächlich zur Kenntnis genommen wird.[163] Die Zugangseröffnung muss für den eingesetzten Dienst jeweils gesondert festgestellt werden.[164]

Durch § 2 Abs. 1 des E-Government-Gesetz des Bundes (EGovG) sind alle vom Anwendungsbereich erfassten Behörden (Bundesbehörden und solche, die Bundesrecht ausführen) verpflichtet, ihrerseits einen Zugang für die Übermittlung elektronischer Dokumente zu schaffen.[165] Die Vorschrift legt die Behörden dabei jedoch nicht auf ein bestimmtes Übermittlungsverfahren fest, sondern ist technikoffen ausgestaltet.[166] Aus dieser behördlichen Verpflichtung folgt jedoch nicht automatisch, dass die Behörde einen solchen Zugang bzw. den vom Bürger im jeweiligen Einzelfall genutzten oder begehrten Kommunikationsweg tatsächlich eröffnet hat.[167] Die Behörde kann z.B. auch bekanntgeben, dass sie bestimmte elektronische Zugangswege nicht nutzt.[168] Eine gesetzliche Zugangsbeschränkung findet sich derzeit in § 87a Abs. 1 Satz 2 AO. Danach ist die Übermittlung elektronischer Nachrichten und Dokumente an Finanzbehörden mit einer qualifizierten elektronischen Signatur oder über das besondere elektronische Behördenpostfach nicht zulässig, soweit für die Übermittlung ein sicheres elektronisches Verfahren der Finanzbehörden zur Verfügung steht, das den Datenübermittler authentifiziert

[161] Schulz, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, Rn. 3a, Rn. 50 ff; BVerwG Urteil vom 07.12.2016 – 6 C 12/15, NVwZ 2017, 967, Rn. 19.
[162] BVerwG, Urteil vom 07.12.2016 – 6 C 12/15, NVwZ 2017, 967, Rn. 19.
[163] VG Köln, Urteil vom 06.12.2024 – 16 K 703/24, BeckRS 2024, 34845, Rn. 17.
[164] Schulz, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, Rn. 3a, Rn. 50.
[165] U. Müller/Dittrich, in: BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.10.2025, § 3a, Rn. 6.
[166] Begründung zu § 2 Abs. 1 EGovG Bund, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 14.11.2012, Drucksache 17/11473, S. 34.
[167] U. Müller/Dittrich, in: BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.10.2025, § 3a, Rn. 10.
[168] Begründung zu § 3a VwVfG n.F., Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 21/3620 – vom 20.05.2026, Drucksache 21/6049, S. 21.

und die Vertraulichkeit und Integrität des Datensatzes gewährleistet. Diese Regelung gilt jedoch nicht für Gerichte und Staatsanwaltschaften sowie in den Fällen, in denen die Übermittlung an Finanzbehörden mit einer qualifizierten elektronischen Signatur oder über das besondere elektronische Behördenpostfach gesetzlich vorgeschrieben ist.

Der in § 2 Abs. 1 EGovG normierten Verpflichtung der Behörden zur Bereitstellung eines elektronischen Zugangs steht auf Seiten der Bürgerinnen und Bürger keine entsprechende Pflicht zur elektronischen Kommunikation gegenüber. Das Verwaltungsverfahrensrecht überlässt es vielmehr der betroffenen Person, ob sie sich auf eine solche Kommunikation mit der Verwaltung einlässt. Eine Pflicht der Bürgerinnen und Bürger zur Entgegennahme elektronischer Dokumente wurde bei den Reformen 2002 und 2013 bewusst nicht geschaffen. Grund war die Erwägung, dass viele Menschen zur elektronischen Kommunikation weder willens noch in der Lage seien und dass die Achtung ihrer Selbstbestimmung sowie der Gleichbehandlungsgrundsatz die Beibehaltung des herkömmlichen Kommunikationswegs geböten. So ist etwa auch die Verwendung des Bürgerkontos im OZG-Kontext gemäß § 3 Abs. 1 Satz 2 OZG für die Nutzer freiwillig ausgestaltet.

An eine konkludente Widmung einer Empfangseinrichtung durch eine Privatperson zum Empfang elektronischer Dokumente von der Verwaltung werden bisher strenge Anforderungen gestellt. Das bloße Vorhalten einer Empfangseinrichtung genügt nicht; von einer Privatperson kann nicht erwartet werden, dass sie sämtliche von ihr unterhaltenen elektronischen Postfächer gewissenhaft überwacht.[169] Auch die Angabe einer E-Mail-Adresse im Briefkopf oder einer Signaturzeile soll nicht genügen.[170] Regelmäßig genügt es demgegenüber, wenn sich die Person selbst elektronisch an die Behörde wendet, wobei sie die Nutzung des Übermittlungswegs auf einen Vorgang oder abgrenzbare Teile beschränken darf.[171] Kennzeichnend bleibt damit stets eine vorangegangene Mitwirkung der betroffenen Person.

Dieser Befund setzt sich auf der Ebene der Bekanntgabe fort. Die elektronische Bekanntgabe eines Verwaltungsakts durch Abruf setzt nach § 41 Abs. 2a VwVfG die Einwilligung des

[169] Müller, Elektronischer Rechtsverkehr im Verwaltungsverfahren, RDi 2024, 162 (164), Rn. 17.
[170] U. Müller/Dittrich, BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.10.2025, § 3a, Rn. 12.
[171] Müller, Elektronischer Rechtsverkehr im Verwaltungsverfahren, RDi 2024, 162 (164), Rn. 17.

Beteiligten voraus. § 9 Abs. 1 OZG lockert dies zwar zu einer Opt-out-Lösung, bei der die Einwilligung als erteilt gilt, knüpft die Bekanntgabe aber an das Postfach des Nutzerkontos und damit an die vorherige Inanspruchnahme einer elektronischen Verwaltungsleistung. Auch die Bekanntgabe durch Bereitstellung zum Datenabruf nach § 122a AO und die Übermittlungsfiktion des § 41 Abs. 2 Satz 2 VwVfG bauen auf einem zuvor eröffneten elektronischen Kanal auf. Ohne vorherige Mitwirkung der Privatperson lässt sich eine wirksame elektronische Bekanntgabe daher nach geltendem Recht nicht bewirken (zu den Regelungen über die elektronische Bekanntgabe von Verwaltungsakten näher 2.2).

Bei Unternehmen und natürlichen Personen, die im beruflichen Kontext auftreten (etwa Freiberuflern), sind dagegen nach der Verkehrsanschauung weniger strenge Anforderungen an eine konkludente Zugangseröffnung zu stellen. So soll etwa bereits die Angabe einer E-Mailadresse außerhalb des Impressums als konkludente Eröffnung des Zugangs für die elektronische Kommunikation genügen.[172]

1.2. Fehlendes Adressregister für Privatpersonen in der ZaPuK-Architektur

Die für ZaPuK vorgesehene Architektur passt technisch zu diesem rechtlichen Befund. Während für Organisationen die Registrierung im Self-Service-Portal (vgl. ADR-0008, ADR-1103 und ADR-1104) und die Verknüpfung der Postfachadresse eines Funktionspostfachs im Adressregister vorgesehen ist, wird für Privatpersonen bewusst kein Adressregister geführt (ADR-1111); die Matrix-Adresse (MXID) wird deterministisch aus einem bereichsspezifischen Pseudonym des jeweiligen Authentisierungsmittels abgeleitet (ADR-1105). Die Adresse entsteht damit erst, wenn die Person sich authentisiert – im Regelfall im Zuge einer Antragstellung, bei der das Pseudonym als Bestandteil des Identitätsnachweises an die Behörde gelangt. Will eine Behörde eine Privatperson proaktiv adressieren, muss die bereichsspezifische Adresse deshalb bereits aus einem früheren Vorgang vorliegen. Liegt sie nicht vor, bedarf es zunächst einer Authentisierung durch die Person selbst (Abschnitt 5.5.2.3 des Konzepts). Die Architektur bildet damit die geltende Rechtslage zutreffend ab: Eine „kalte" Kontaktaufnahme mit einer Person, die noch nie elektronisch mit der Verwaltung interagiert hat, ist rechtlich nicht zulässig und

[172] U. Müller/Dittrich, BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.10.2025, § 3a, Rn. 12.

technisch grundsätzlich nicht möglich. Diese Zurückhaltung ist zugleich datenschutzrechtlich vorzugswürdig, weil ein zentrales, für die proaktive Adressierung aller Bürgerinnen und Bürger geeignetes Register erhebliche Risiken einer staatlichen oder – im Fall einer Kompromittierung – nichtstaatlichen Profilbildung begründen würde (siehe D.III.3.3.3.a).

1.3. Neuordnung durch das Gesetz für den Bürokratierückbau zum 1. Juli 2027

Das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 3. Juli 2026 ordnet die Vorschriften zur elektronischen Kommunikation neu. Der zum 1. Juli 2027 in Kraft tretende § 3a Abs. 1 VwVfG in der neuen Fassung bestimmt, dass die Kommunikation zwischen Behörden und Beteiligten elektronisch erfolgen „soll".[173] Dies gilt ausweislich der Gesetzesbegründung unabhängig davon, ob es sich um eine juristische Person oder natürliche Person handelt. Der Begriff des „Beteiligten" ist dabei nach der Gesetzesbegründung weit zu verstehen und reicht über § 13 Abs. 1 VwVfG hinaus. Erfasst sind auch informelle Auskunftsanfragen und die bloße Übersendung von Informationen im Vorfeld eines Verwaltungsverfahrens.[174] Die Vorschrift verschiebt damit die programmatische Ausrichtung von der herkömmlichen zur elektronischen Kommunikation.

Dieser Perspektivwechsel trägt die proaktive Zustellung ohne Mitwirkung der betroffenen Person gleichwohl nicht. Das ergibt sich nicht nur aus dem Wortlaut, sondern auch ausdrücklich aus der Gesetzesbegründung. Erstens ist die Norm bewusst als Soll-Vorschrift ausgestaltet, weil es Fälle geben kann, in denen die Kommunikation nur auf anderem Weg als elektronisch erfolgen kann – die Begründung nennt Härtefälle aufgrund körperlicher Beeinträchtigungen oder fortgeschrittenen Alters. Zweitens – und für die hier maßgebliche Frage entscheidend – hält der Gesetzgeber an der Zugangseröffnung durch die Privatperson ausdrücklich fest: Da noch keine allgemeine Verpflichtung bestehe, dem Staat eine digitale Adresse mitzuteilen, bleibe für den elektronischen Rechtsverkehr mit Behörden eine elektronische Zugangseröffnung seitens der Privatperson weiterhin erforderlich. Diese könne zwar niederschwellig erfolgen, etwa durch

[173] Art. 1 Nr. 3 Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern.
[174] Begründung zu § 3a VwVfG n.F., Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 21/3620 – vom 20.05.2026, Drucksache 21/6049, S. 21.

Angabe einer E-Mail-Adresse in einem Dokument; Privatpersonen könnten sich aber weiterhin gegen die elektronische Kommunikation entscheiden und auf den postalischen Weg verweisen. Die Soll-Vorschrift adressiert damit das behördliche Verhalten bei bereits eröffnetem Zugang – „auf eine elektronische Eingabe antwortet die Behörde grundsätzlich auch elektronisch"[175] –, begründet aber keine einseitige Befugnis zur elektronischen Erstansprache.

Drittens lässt die Reform die maßgeblichen Bekanntgaberegeln grundsätzlich unberührt: § 41 VwVfG wird nicht geändert, sodass die Bekanntgabe durch Abruf weiterhin die Einwilligung des Beteiligten voraussetzt (§ 41 Abs. 2a VwVfG), und auch § 9 OZG sowie § 122a AO bleiben unverändert an das Nutzerkonto beziehungsweise die Bereitstellung zum Abruf gebunden. Viertens beseitigt die Reform die technische Hürde der fehlenden Adresse nicht. Die Reform bekräftigt damit im Ergebnis das Fortbestehen des Freiwilligkeitsprinzips und schafft keine Grundlage für eine allgemeine, einwilligungslose proaktive Adressierung von Privatpersonen. Sie unterstreicht vielmehr, dass hierfür eine gesonderte gesetzliche Entscheidung des Gesetzgebers erforderlich ist.

1.4. Sinnvolle Rechtsänderungen

Soll die proaktive digitale Zustellung an Privatpersonen über den Fall der zuvor eröffneten Erreichbarkeit hinaus allgemein ermöglicht werden, empfiehlt sich eine ausdrückliche spezialgesetzliche Grundlage. Sie sollte drei Elemente verbinden: Erforderlich ist zunächst eine Ermächtigung mit einer klar geregelten Zugangs- beziehungsweise Bekanntgabefiktion nach dem Vorbild des § 9 Abs. 1 OZG und des § 122a AO, die den Anwendungsbereich auf bestimmte Verfahren und Nachrichtentypen begrenzt und die Beweislast für die Bereitstellung – wie dort – der Behörde zuweist. Erforderlich ist ferner eine tragfähige Lösung für die Adressverfügbarkeit, die den bewussten Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111) nicht unterläuft. Vorzugswürdig ist ein Opt-in-Mechanismus, mit dem eine Person ihre Erreichbarkeit für einen Bereich einmalig und widerruflich aktiviert, verbunden mit einer Benachrichtigung über einen zweiten Kanal. Erforderlich ist schließlich die Sicherstellung der tatsächlichen

[175] Begründung zu § 3a VwVfG n.F., Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 21/3620 – vom 20.05.2026, Drucksache 21/6049, S. 21.

Kenntnisnahmemöglichkeit: Eine Fiktion, die an die bloße Bereitstellung anknüpft, ist nur tragfähig, wenn die bereitgestellte Nachricht für die Person auch lesbar ist; die funktionierende Schlüsselwiederherstellung ist deshalb zugleich Voraussetzung eines rechtssicheren fingierten Zugangs (siehe dazu näher III.3.6.2.e) und VII.1). Aus Gründen der Gleichbehandlung – die auch die Gesetzesbegründung zur Soll-Vorschrift des § 3a Abs. 1 VwVfG n.F. leitet – ist eine Rückfallebene für nicht digital erreichbare Personen vorzusehen.

1.5. Folgerungen für die Architektur von ZaPuK

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Die elektronische Kommunikation über ZaPuK setzt voraus, dass der jeweilige Empfänger diesen Kommunikationskanal ausdrücklich oder zumindest konkludent als elektronischen Zugangsweg eröffnet hat oder eine spezielle gesetzliche Regelung die Nutzung von ZaPuK explizit anordnet.

- Legt man das in der Gesetzesbegründung zu § 3a VwVfG n.F. zum Ausdruck kommende Verständnis zugrunde, entwickelt sich die Verkehrsauffassung dahin, dass die konkludente Zugangseröffnung im Privatbereich – wie auch im unternehmerischen Kontext – künftig niedrigschwellig ausfällt.

- Nach diesem Verständnis ist davon auszugehen, dass die konkludente Zugangseröffnung für ZaPuK durch Antragstellung erfolgt, wenn eine Postfachadresse eines Funktionspostfachs durch eine Organisation oder das bereichsspezifische Pseudonym einer Privatperson, aus dem die MXID der Privatperson dynamisch abgeleitet werden kann (ADR-1105), als Rückantwortadresse angegeben wird (vgl. Abschnitt 5.1, 5.5.2 und 5.5.2.1 des Konzepts).

- Für einen proaktiven digitalen Schriftverkehr gegenüber Organisationen erscheint die Registrierung der Organisation im Self-Service-Portal (vgl. ADR-0008, ADR-1103 und ADR-1104) mit Verknüpfung der Postfachadresse eines Funktionspostfachs im Adressregister (ADR 1111) als konkludente Zugangseröffnung denkbar (vgl. Abschnitt 5.1, 5.4.6 und 5.5.1.1 des Konzepts).

- Die Grundentscheidung, eine proaktive Kontaktaufnahme von Privatpersonen nur bei bereits vorliegender, aus einem früheren Vorgang abgeleiteter Adresse zuzulassen und andernfalls eine vorherige Authentisierung zu verlangen (Abschnitt 5.5.2.3 des Konzepts), bildet die geltende Rechtslage – auch nach der Reform des § 3a VwVfG – zutreffend ab.

- Der Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111) und die pseudonyme, bereichsspezifische Adressierung (ADR-1105) sind auch mit Blick auf eine mögliche proaktive Kontaktaufnahme vorzugswürdig (zur Datenminimierung siehe D.III.3.3.3.a)) und sollten nicht durch ein zentrales Register ersetzt werden. Wird die proaktive Adressierung künftig gesetzlich ermöglicht, wäre ein nutzergesteuerter Opt-in-Mechanismus zur bereichsbezogenen Aktivierung der Erreichbarkeit eine datenschutzkonforme Erweiterung.

2. Erklärungen/Nachrichten von Seiten der Behörde

2.1. Begriffliche Grundlagen – Zugang, Bekanntgabe, Zustellung

Kurzzusammenfassung: Ausgangspunkt für die Bestimmung des Zeitpunkts, zu dem eine Erklärung ihrem Empfänger gegenüber rechtliche Wirkung entfaltet, sind die allgemeinen (zivilrechtlichen) Grundsätze über den **Zugang empfangsbedürftiger Willenserklärungen**. Der Zugang setzt voraus, dass die Erklärung so in den Machtbereich des Empfängers gelangt ist, dass dieser unter normalen Verhältnissen die Möglichkeit hat, vom Inhalt der Erklärung Kenntnis zu nehmen. Für den Bereich des Steuerverwaltungsverfahrensrechts regelt § 87a Abs. 1 AO ausdrücklich, dass ein elektronisches Dokument zugegangen ist, sobald die für den Empfang bestimmte Einrichtung es in für den Empfänger bearbeitbarer Weise aufgezeichnet hat.

Die **Bekanntgabe eines Verwaltungsakts** ist die vom Willen der Behörde getragene, amtlich veranlasste Eröffnung des Verwaltungsakts. Erst mit der Bekanntgabe wird der Verwaltungsakt rechtlich existent und wirksam. Grundsätzlich setzt auch die Bekanntgabe den Zugang des Verwaltungsakts voraus. Allerdings enthält das Verwaltungsverfahrensrecht besondere

Bekanntgabe- bzw. Zugangsfiktionen, die die rechtssicherere Bestimmung des für den Beginn von Rechtsbehelfsfristen maßgeblichen Zeitpunkts erleichtern sollen.

Bei der **Zustellung** handelt es sich demgegenüber um die Bekanntgabe eines Dokuments in einer gesetzlich besonders geregelten, formgebundenen Art und Weise. Auf Bundesebene richtet sich die förmliche Zustellung nach den Vorschriften des VwZG.

Nach allgemeinen (zivilrechtlichen) Grundsätzen ist der Zugang einer Willenserklärung (2.1.1) entscheidend für deren rechtliche Wirksamkeit. Im verwaltungsrechtlichen Kontext werden diese überlagert und modifiziert durch die Regelungen zur Bekanntgabe von Verwaltungsakten (2.1.2) sowie – soweit anwendbar – zur förmlichen Zustellung (2.1.3).

2.1.1. Zugang einer Willenserklärung

Nach der zivilrechtlichen Bestimmung in § 130 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB) wird eine Willenserklärung, die einem anderen gegenüber abzugeben ist, wenn sie in dessen Abwesenheit abgegeben wird, in dem Zeitpunkt wirksam, in welchem sie ihm zugeht. Vom Zugang einer solchen Willenserklärung ist nach ständiger Rechtsprechung des Bundesgerichtshofs (BGH) dann auszugehen, wenn sie so in den Machtbereich des Empfängers gelangt ist, dass dieser unter normalen Verhältnissen die Möglichkeit hat, vom Inhalt der Erklärung Kenntnis zu nehmen.[176]

Auch im Verwaltungsverfahrensrecht wird entsprechend auf die zu § 130 BGB entwickelten Grundsätze zum Wirksamwerden empfangsbedürftiger Willenserklärungen zurückgegriffen, soweit die öffentlich-rechtlichen Bestimmungen keine Sonderregelungen aufstellen.[177]

Für den Bereich des Steuerverwaltungsverfahrensrechts bestimmt § 87a Abs. 1 Satz 3 Halbsatz 1 AO ausdrücklich, dass ein elektronisches Dokument zugegangen ist, sobald die für den Empfang bestimmte Einrichtung es in für den Empfänger bearbeitbarer Weise aufgezeichnet hat.

[176] Siehe etwa BGH, Urteil vom 22.10.2024 – II ZR 64/23, ZPG 2025, 26, Rn. 18.
[177] U. Stelkens, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 41, Rn. 7 f.

Ob und wann der Empfänger das Dokument an seinem Bildschirm aufruft oder sich ausdrucken lässt, ist nach den Gesetzesmaterialien zu § 87a Abs. 1 AO nicht maßgeblich.[178]

2.1.2. Bekanntgabe von Verwaltungsakten

Die Bekanntgabe von Verwaltungsakten (Bescheiden) ist die vom Willen der erlassenden Behörde getragene, amtlich veranlasste Eröffnung des Verwaltungsakts.[179] Bei ihr handelt es sich um den abschließenden Verfahrensschritt des auf den Erlass eines Verwaltungsakts gerichteten Verwaltungsverfahrens. Erst mit der Bekanntgabe erlangt ein Verwaltungsakt rechtliche Existenz und entfaltet Wirksamkeit (siehe §§ 41 Abs. 1 und 43 Abs. 1 VwVfG, §§ 122 Abs. 1 und 124 Abs. 1 AO sowie §§ 37 Abs. 1 und 39 SGB X).[180]

Die Bekanntgabe stellt sich grundsätzlich als mehraktiger Vorgang dar. Zunächst muss sich die Behörde des Verwaltungsakts entäußern, ihn also – vergleichbar mit der Abgabe einer Willenserklärung – aus ihrem internen Verantwortungsbereich entlassen. Hierdurch allein ist der Verwaltungsakt jedoch noch nicht bekannt gegeben. Die Bekanntgabe setzt dem Grundsatz nach in analoger Anwendung des § 130 BGB den Zugang des Verwaltungsakts voraus.[181] Der Verwaltungsakt muss also so in den „Machtbereich" des Empfängers gelangen, dass bei gewöhnlichem Verlauf und normaler Gestaltung der Verhältnisse des Empfängers mit der Kenntnisnahme durch ihn zu rechnen ist.[182] Auf die tatsächliche Kenntnisnahme kommt es dabei jedoch nicht an.[183] Wann Verfügungsgewalt über eine Datei erlangt worden ist, bestimmt sich nach der Verkehrsauffassung.[184]

---

[178] Begründung zu § 87a AO, Gesetzentwurf der Bundesregierung, Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 13.05.2002, Drucksache 14/9000, S. 36.
[179] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 17.
[180] U. Stelkens, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 41, Rn. 1 ff.
[181] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 18 und 73.
[182] BVerwG, Beschluss vom 21.12.2017 – 6 B 43/17, NVwZ 2018, 496, Rn. 11.
[183] Tiedemann, in: BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.04.2026, § 41, Rn. 8.
[184] Baer/Wiedmann, in: Schoch/Schneider, Verwaltungsrecht – VwVfG, Werkstand: 7. EL Mai 2025, § 41, Rn. 66.

Die Vorschriften über die Bekanntgabe enthalten gesetzliche Bekanntgabe- bzw. Zugangsfiktionen. Diese dienen in erster Linie der rechtssicheren Berechnung von Rechtsbehelfsfristen, indem ein möglicher Streit über den Zeitpunkt des tatsächlichen Zugangs durch eine gesetzliche Fiktion ersetzt wird.[185] Dadurch gewährleisten sie Rechtsklarheit hinsichtlich des Beginns von Rechtsbehelfsfristen und tragen zugleich zur Verwaltungsvereinfachung bei, da sich der tatsächliche Zugang in der Praxis häufig nur schwer nachweisen lässt.[186] Die gesetzlichen Fiktionen beruhen nicht auf einem verallgemeinerungsfähigen Rechtsgedanken und sind daher einer analogen Anwendung nicht zugänglich.

Fehlt es in den jeweils maßgeblichen Sachregelungen an einer Bestimmung über die Art und Weise der Bekanntgabe des Verwaltungsakts, steht die Wahl der Bekanntgabeform grundsätzlich im Ermessen der Behörde. Allerdings muss die Bekanntgabe einer hoheitlichen Maßnahme, durch die dem Bürger seine rechtliche Betroffenheit mitgeteilt und durch die eine Frist in Gang gesetzt wird, nach deren Ablauf die Maßnahme Bestandskraft erlangt, den Anforderungen des durch Art. 19 Abs. 4 GG gewährleisteten effektiven Rechtsschutzes genügen. Sie muss ferner geeignet sein, der Verwirklichung des Anspruchs auf rechtliches Gehör gemäß Art. 103 Abs. 1 GG zu dienen.[187]

2.1.3. Zustellung

Die Zustellung ist die Bekanntgabe eines Dokuments in einer gesetzlich bestimmten, formgebundenen Art und Weise. Sinn dieser strengen Formbindung ist es, rechtssicher den Zeitpunkt der Bekanntgabe nachweisen zu können und den tatsächlichen Zugang des Dokuments zu gewährleisten. Das Rechtsinstitut der Zustellung beschränkt sich nicht nur auf Verwaltungsakte, sondern erfasst alle Arten von Dokumenten, die behördliche Erklärungen beinhalten. Auf die Rechtsnatur des Inhalts kommt es dabei nicht an.[188]

[185] Vgl. Tiedemann, in: BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.04.2026, § 4, Rn. 62.
[186] Vgl. BVerwG, Urteil vom 29.11.2023 – 6 C 3.22, NVwZ 2024, 746, Rn. 20 f.
[187] BVerwG, Beschluss vom 21.12.2017 – 6 B 43/17, NVwZ 2018, 496, Rn. 11.
[188] Preisner, in: BeckOK OWiG, Graf, 51. Edition, Stand: 01.07.2026, § 1 VwZG, Rn. 1 und § 2 VwZG, Rn. 1 und 5; § 2 Abs. 1 VwZG des Bundes definiert die „Zustellung" als die Bekanntgabe eines schriftlichen oder elektronischen Dokuments in der im VwZG des Bundes bestimmten Form.

Förmlich zugestellt wird auf Bundesebene nach dem VwZG (gilt nach § 122 Abs. 5 Satz 2 AO auch für den Bereich der Steuerverwaltung sowie nach § 65 Abs. 1 SGB X für den Bereich der Sozialverwaltung), soweit dies durch Rechtsvorschrift oder behördliche Anordnung bestimmt ist (§§ 1 Abs. 2 VwZG, 122 Abs. 5 Satz 1 AO).

Dies ist im VwVfG des Bundes etwa bei Verwaltungsakten der Fall, die das förmliche Verfahren abschließen (§ 69 Abs. 2 Satz 1 VwVfG), oder bei Planfeststellungsbeschlüssen (§ 74 Abs. 4 Satz 1 VwVfG). Auch bei Widerspruchsbescheiden im Sinne der Verwaltungsgerichtsordnung (VwGO) ist eine formelle Zustellung Pflicht.[189]

Auch das Zustellungsrecht enthält besondere Fiktionsregelungen, die bei verweigerter Mitwirkung an der Zustellung greifen.

2.2. Digitale Bekanntgabe von Verwaltungsakten

Kurzzusammenfassung: Die Verfahrensordnungen des Bundes (VwVfG, SGB X, AO) sowie das OZG sehen nach aktueller Gesetzeslage unterschiedliche Bekanntgabe- und Fiktionsmodelle für Verwaltungsakte vor. Systematisch lässt sich dabei im Wesentlichen zwischen den Vorschriften über die elektronische Übermittlung und den Vorschriften über die Bereitstellung zum Abruf unterscheiden. Nach der aktuellen Konzeption dürften – vorbehaltlich einer speziellen Regelung für ZaPuK – beide Modelle für die ZaPuK-Infrastruktur relevant sein, je nachdem ob es sich um ein zentral oder dezentral betriebenes Empfänger-Backend handelt.

Welche Anforderungen an die wirksame Bekanntgabe eines Verwaltungsakts zu stellen sind, hängt nach der derzeitigen Gesetzeslage von der Art der behördlichen Entscheidung und den jeweils einschlägigen verfahrensrechtlichen Vorschriften ab.[190] Für die elektronische Bekanntgabe von Verwaltungsakten sehen die verschiedenen Verfahrensordnungen des Bundes – das

[189] Das Widerspruchsverfahren richtet sich im Anwendungsbereich der VwGO nach den §§ 68 ff. VwGO. Gemäß § 73 Abs. 3 Satz 1 und 2 VwGO sind Widerspruchsbescheide von Amts wegen nach den Vorschriften des VwZG zuzustellen. Nach § 85 Abs. 3 Satz 1 Sozialgerichtsgesetz (SGG) ist der Widerspruchsbescheid den Beteiligten lediglich bekanntzugeben. Nimmt die Behörde aber eine Zustellung vor, gelten nach § 85 Abs. 3 Satz 2 SGG ebenso die §§ 2 bis 10 des VwZG.

[190] BVerwG, Beschluss vom 21.12.2017 – 6 B 43/17, NVwZ 2018, 496, Rn. 10.

VwVfG, das SGB X und die AO – sowie auch das OZG derzeit unterschiedliche Bekanntgabe- bzw. Fiktionsmodelle vor. Dabei lässt sich im Wesentlichen zwischen den Vorschriften über die elektronische Übermittlung des Verwaltungsakts nach den §§ 41 Abs. 2 VwVfG, 37 Abs. 2 Satz 2 SGB X und 122 Abs. 2a AO – etwa durch Übermittlung an ein E-Mail-Postfach des Adressaten – und den Bestimmungen über den Abruf über öffentlich zugängliche Netze/der Bereitstellung zum (Daten-)Abruf nach den §§ 41 Abs. 2a VwVfG, 9 Abs. 1 OZG, 122a AO sowie 37 Abs. 2a und Abs. 2b SGB X – etwa über Behördenportale, die zentral bereitgestellten OZG-Postfächer oder ELSTER – unterscheiden. Während die Vorschriften über die elektronische Übermittlung in Anlehnung an die postalische Bekanntgabe auf dem Gedanken beruhen, dass der Verwaltungsakt durch den erfolgreichen Transfer in den Machtbereich des Empfängers gelangt, scheinen die Vorschriften über den Abruf bzw. die Bereitstellung zum (Daten-)Abruf eher auf dem Verständnis zu basieren, dass der Verwaltungsakt zunächst in einem behördenseitig verantworteten Postfach oder Portal bereitgestellt und von dort durch den Berechtigten abgeholt wird. Inwieweit solche staatlich verantworteten Abrufumgebungen dem Machtbereich des Empfängers zugeordnet werden können, ist fraglich und noch nicht abschließend geklärt.

Nach derzeitiger Rechtslage ist daher davon auszugehen, dass für ZaPuK beide Kategorien von Bekanntgabemodellen relevant sind. Dabei ist zwischen den unterschiedlichen Betriebsmodellen der Postfachinfrastruktur – also dem dezentralen und dem zentralen Betrieb des Empfänger-Backends – zu differenzieren:

Während bei einem dezentralen, eigenverantwortlichen Betrieb des Empfänger-Backends nach aktueller Gesetzeslage die Annahme eines elektronischen Übermittlungsvorgangs im Sinne der §§ 41 Abs. 2 VwVfG, 37 Abs. 2 Satz 2 SGB X und 122 Abs. 2a AO nahe liegt (siehe hierzu 2.2.1), erscheint bei einem elektronischen Datentransfer in ein zentrales, durch eine staatliche Stelle betriebenes Backend nach aktueller Gesetzeslage die Anwendung der Vorschriften über die Bekanntgabe durch Abruf bzw. durch Bereitstellung zum (Daten-)Abruf über öffentlich zugängliche Netze nach § 41 Abs. 2a VwVfG bzw. – unter der Voraussetzung, dass das OZG-Postfach von den OZG-Nutzerkonten entkoppelt wird – § 9 Abs. 1 OZG sowie den § 122a AO, § 37 Abs. 2a und Abs. 2b SGB X geboten (siehe hierzu D.II.2.2.2).

Vorbehaltlich einer speziellen gesetzlichen Regelung, die für die Bekanntgabe über ZaPuK einheitlich an die qualifizierte Abrufumgebung der ZaPuK-Infrastruktur anknüpft, richten sich die Anforderungen an die Nachweisführung und die hierfür erforderlichen technischen und funktionalen Eigenschaften des Systems folglich nach dem jeweils einschlägigen Bekanntgabemodell.

2.2.1. Elektronische Übermittlung an den Empfänger – dezentraler Backend-Betrieb bei Organisationspostfächern

Kurzzusammenfassung: Bei dezentral und eigenverantwortlich betriebenen Empfänger-Backends für Organisationspostfächer (Option C; zu den Anschlussbedingungen siehe D.VII.3) ist – vorbehaltlich einer spezielleren Regelung, die an die qualifizierte Abrufumgebung des ZaPuK-Verbunds anknüpft – davon auszugehen, dass sich die Bekanntgabe im Wesentlichen nach den Vorschriften über die elektronische Übermittlung (§ 41 Abs. 2 VwVfG, § 37 Abs. 2 SGB X, § 122 Abs. 2a AO) richtet.

Danach muss die Behörde in Zweifelsfällen den Zugang und den Zugangszeitpunkt des elektronischen Dokuments nachweisen können. Die Systemfunktionen von ZaPuK müssen hierfür abbilden können, ob und wann das übermittelte elektronische Dokument abrufbar auf dem Empfänger-Backend gespeichert worden ist; auf den tatsächlichen Abruf durch den Empfänger kommt es hingegen nicht an. Anhand der in der ZaPuK-Architektur vorgesehenen automatischen serverseitigen Bereitstellungsbestätigung (ADR-0018) kann nachvollzogen werden, ob und zu welchem Zeitpunkt die Nachricht das Empfänger-Backend erreicht hat. Die Bereitstellungsbestätigung belegt allerdings nicht, dass die Nachricht durch den Empfänger entschlüsselt und gelesen werden kann. Um das Risiko einer unwirksamen Bekanntgabe zu reduzieren, sollte die Infrastruktur daher so ausgestaltet werden, dass Verschlüsselungsfehler verhindert oder revisionssicher dokumentiert werden (siehe hierzu D.VII.1). Zur Beweiskraft der Bereitstellungsbestätigung siehe ferner D.VI.2.2.

Werden Anhänge nicht zusammen mit der Nachricht übertragen, sondern vom Empfänger-Backend automatisiert, proaktiv aus dem Absender-Backend abgerufen, spricht Überwiegendes dafür, auch diesen Vorgang als elektronische Übermittlung im Sinne der genannten

Vorschriften einzuordnen. Verbleiben die Anhänge dagegen bis zum aktiven Abruf durch den Empfänger im Media-Repository des Absender-Servers (Pull-Prinzip), ist von einem Abruf-/Bereitstellungsmodell auszugehen (siehe 2.2.2).

Für das Steuerverwaltungsverfahren ist nach §§ 122 Abs. 2a i.V.m. 87a Abs. 7 AO ein sicheres Verfahren erforderlich, das die übermittelnde Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet. Im Gesetz wird beispielhaft die Verwendung einer qualifizierten elektronischen Signatur zusammen mit einem geeigneten Verschlüsselungsverfahren genannt. Hieraus folgt jedoch nicht, dass ZaPuK selbst Funktionen zur Erzeugung qualifizierter elektronischer Signaturen oder Siegel bereitstellen muss. Es genügt insoweit, wenn ZaPuK den unveränderten Transport von Dokumenten ermöglicht, die der jeweilige Absender zuvor eigenverantwortlich signiert oder gesiegelt hat (vgl. ADR-0017, Abschnitt 5.4.12 und 5.5.4 des Konzepts). Zu den konkreten Anforderungen des datenschutzrechtlichen Grundsatzes der Integrität und Vertraulichkeit siehe D.III.3.6.

Nach der aktuellen Konzeption von ZaPuK sind Organisationen nicht auf die Nutzung eines zentralen Postfach-Backends beschränkt. Sie können stattdessen – unter Einhaltung der Anschlussbedingungen (siehe hierzu D.VII.3) – auch eigene Backends in eigener Verantwortung dezentral betreiben (Option C; ADR-1103, Abschnitt 5.6 des Konzepts). In diesem Fall kann davon ausgegangen werden, dass sich die Bekanntgabe von Verwaltungsakten im Wesentlichen nach den Bestimmungen der §§ 41 Abs. 2 VwVfG, 37 Abs. 2 SGB X oder 122 Abs. 2a AO zur elektronischen Übermittlung richtet.

a) Übermittlung nach §§ 41 Abs. 2 VwVfG, 37 Abs. 2 SGB X oder 122 Abs. 2a AO

Wird ein Bescheid elektronisch nach den §§ 41 Abs. 2 VwVfG, 37 Abs. 2 Satz 2 SGB X oder 122 Abs. 2a AO übermittelt, gilt eine **Vier-Tage-Fiktion für die Bekanntgabe**.

§ 41 Abs. 2 VwVfG bestimmt für das allgemeine Verwaltungsverfahrensrecht wie folgt:

> *[1]Ein schriftlicher Verwaltungsakt, der im Inland durch die Post übermittelt wird, gilt am vierten Tag nach der Aufgabe zur Post als bekannt gegeben. [2]Ein Verwaltungsakt, der im Inland oder in das Ausland elektronisch übermittelt wird,*

> *gilt am vierten Tag nach der Absendung als bekannt gegeben. [3]Dies gilt nicht, wenn der Verwaltungsakt nicht oder zu einem späteren Zeitpunkt zugegangen ist; im Zweifel hat die Behörde den Zugang des Verwaltungsaktes und den Zeitpunkt des Zugangs nachzuweisen.*
>
> (Hervorhebung hier hinzugefügt)

Die Vorschrift enthält sowohl eine – im Streitfall nicht relevante – gesetzliche Fiktion, wonach der Verwaltungsakt nicht vor dem genannten Zeitpunkt als zugegangen gilt, als auch eine widerlegliche Vermutung der Bekanntgabe. Voraussetzung für das Eingreifen dieser Vermutung ist der nachweisliche tatsächliche Ausgang des Bescheids bei der Behörde.[191]

Für den Fall, dass der Empfänger des elektronisch übermittelten Verwaltungsakts den Zugang bestreitet, gelten nach § 41 Abs. 2 Satz 3 VwVfG für das Bestreiten und die Verteilung der Beweislast dieselben Grundsätze wie auch beim postalisch übermittelten schriftlichen Verwaltungsakt.[192] Bestehen Zweifel am Zugang – hält die Behörde oder das Gericht den Zugang also für ungewiss – oder bestehen Zweifel am Zugangszeitpunkt, ist die Behörde nachweispflichtig.[193]

In der Rechtsprechung hat sich für den Zugang von E-Mails die Auffassung durchgesetzt, dass es **aus der technischen Perspektive** maßgeblich ist, dass die E-Mail auf dem Mailserver des Empfängers bzw. seines Providers eingegangen und für den Empfänger abrufbar gespeichert ist.[194] Nicht erforderlich sei es hingegen, dass der Empfänger die E-Mail tatsächlich über sein

---

[191] Vgl. BVerwG, Urteil vom 29.11.2023 – 6 C 3.22, NVwZ 2024, 746, Rn. 20 f. zur postalischen Übermittlung schriftlicher Verwaltungsakte.

[192] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 96.

[193] Vgl. BVerwG, Urteil vom 29.11.2023 – 6 C 3.22, NVwZ 2024, 746, Rn. 23 f. zur postalischen Übermittlung schriftlicher Verwaltungsakte; zur Darlegung von Zweifeln genügt hiernach regelmäßig das einfache Bestreiten des Zugangs, weil einem Adressaten, der den Zugang überhaupt bestreitet – anders als bei einem verspäteten Zugang – eine weitere Substantiierung typischerweise nicht möglich ist. Bestreitet der Adressat den Zugang, haben die Behörde bzw. das Gericht die Glaubhaftigkeit seines Vortrags und seine Glaubwürdigkeit zu würdigen.

[194] Siehe BSG, Urteil vom 11.07.2019 – B 14 AS 51/18 R, BeckRS 2019, 20519, Rn. 30; BGH, Urteil vom 06.10.2022 - VII ZR 895/21, ZfBR 2023, 42, Rn. 20; LSG Sachsen, Urteil vom 12.10.2023 – L 3 AS 1050/19, BeckRS 2023, 39454, Rn. 35; BFH, Urteil vom 29.4.2025 – VI R 2/23, NJW 2025, 3317, Rn. 11.

E-Mail-Programm (etwa Outlook oder Apple Mail) abruft.[195] Unerheblich sei auch, ob ein vom Empfänger eingesetzter Spamfilter die E-Mail innerhalb des Postfachs in den Spamordner einsortiere.[196] Die in der Rechtsprechung zum Zugang von einfachen E-Mails zum Ausdruck kommende Verkehrsauffassung erscheint auf Organisationspostfächer, die im ZaPuK-Verbund auf eigenen, dezentral betriebenen Backends in der Verantwortung der jeweiligen Organisationen geführt werden (Option C), ohne Weiteres übertragbar. Es ist jedenfalls nicht ersichtlich, weshalb für den Zugang zu derartigen Postfächern strengere Maßstäbe gelten sollten als für den Zugang zu herkömmlichen E-Mails.

Der Zugang scheidet jedenfalls aus, wenn die Datei aus Gründen, die im Verantwortungsbereich der Behörde liegen, nicht lesbar ist, etwa wenn die übermittelte Datei korrupt – also fehlerhaft – ist und daher vom Empfänger nicht geöffnet bzw. gelesen werden kann.[197]

Die Regelung des § 41 Abs. 2 VwVfG findet sich inhaltsgleich sowohl in § 37 Abs. 2 Satz 2 SGB X für das Sozialverwaltungsverfahrensrecht (dort im Wortlaut beinahe identisch) als auch in § 122 Abs. 2a AO für das Steuerverwaltungsverfahrensrecht wieder.

b) Besonderheiten im Bereich der Steuerverwaltung

Für den Bereich der Steuerverwaltung ist zusätzlich die Regelung des § 87a Abs. 7 AO zu beachten, die für die Übermittlung elektronisch erlassener Verwaltungsakte nach § 122 Abs. 2a AO die **Verwendung eines sicheren Verfahrens** vorschreibt, das die übermittelnde Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet (§ 87a Abs. 7 Satz 1 AO).

§ 87a Abs. 7 Satz 2 AO verweist insofern beispielhaft – jedoch nicht abschließend –[198] auf die Verwendung einer **qualifizierten elektronischen Signatur** im Sinne des Art. 3 Nr. 12 der sog.

[195] Siehe VG München, Urteil vom 14.08.2025 – M 23 K 24.5464, BeckRS 2025, 36985, Rn. 58; VG Minden, Urteil vom 09.06.2026 – 3 K 1209/23, BeckRS 2026, 13206, Rn. 47 f.
[196] Siehe OVG NRW, Beschluss vom 23.09.2021 – 9 B 947/21, BeckRS 2021, 30471, Rn. 3; VG Münster, Urteil vom 15.07.2024 – 9 K 2398/23, BeckRS 2024, 29535, Rn. 23.
[197] Tiedemann, in: BeckOK VwVfG, Bader/Ronellenfitsch, 71. Edition, Stand: 01.04.2026, § 41, Rn. 23.
[198] Hahlweg, in: Koenig, Abgabenordnung, 6. Auflage 2026, § 87a, Rn. 65.

eIDAS-Verordnung (eIDAS-VO)[199] und den Einsatz eines **geeigneten Verschlüsselungsverfahrens** *(„Ein sicheres Verfahren liegt insbesondere vor, wenn der Verwaltungsakt mit einer qualifizierten elektronischen Signatur versehen und mit einem geeigneten Verfahren verschlüsselt ist.").*[200]

Der Einsatz eines geeigneten Verschlüsselungsverfahrens ist auch bei der Übermittlung sonstiger elektronischer Dokumente ohne Verwaltungsaktqualität relevant, wenn diese Daten enthalten, die dem Steuergeheimnis im Sinne des § 30 AO (siehe hierzu auch D.III.1.2.3.b)) unterliegen. § 87a Abs. 1 Satz 4 AO stellt insoweit klar, dass solche, von der Finanzbehörde übermittelten Daten mit einem geeigneten Verfahren zu verschlüsseln sind und auf eine solche Verschlüsselung nur verzichtet werden kann, soweit alle betroffenen Personen schriftlich eingewilligt haben.

c) Folgerungen für die Architektur von ZaPuK

- Werden Organisationspostfächer auf eigenen, dezentral betriebenen Backends in der Verantwortung der jeweiligen Organisationen geführt (Option C), kann jedenfalls **aus technischer Perspektive** – vorbehaltlich der Frage, an welchem Tag oder zu welcher Uhrzeit der Adressat unter gewöhnlichen Verhältnissen die Möglichkeit hat, vom Inhalt der übermittelten Erklärung Kenntnis zu nehmen – dann von einem Zugang eines elektronischen Verwaltungsakts ausgegangen werden, wenn die Datei auf dem Empfänger-Backend eingegangen und für den Empfänger abrufbar gespeichert ist. Auf einen tatsächlichen Abruf der Nachricht kommt es insofern nicht an. Dies gilt auch für andere Erklärungen der Behörde auf die die gesetzliche Fiktion und die

[199] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

[200] Durch die in Art. 15 Abs. 6 Nr. 2 lit. d des Gesetzes für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 03.07.2006 enthaltene Änderung ist die Möglichkeit entfallen, den Verwaltungsakt mit einer De-Mail-Nachricht nach § 5 Abs. 5 des De-Mail-Gesetzes zu versenden, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Finanzbehörde als Nutzer des De-Mail-Kontos erkennen lässt.

Bekanntgabevermutung aus den §§ 41 Abs. 2 VwVfG, 37 Abs. 2 SGB X oder 122 Abs. 2a AO keine Anwendung findet.

- Für eine rechtssichere Bekanntgabe nach dem Übermittlungsmodell muss ZaPuK Systemfunktionen bereitstellen, die der Behörde den Nachweis der Versendung und im Zweifel auch den Nachweis des Zugangs und seines Zeitpunktes ermöglichen:

- Positiv ist vor diesem Hintergrund zu bewerten, dass in der ZaPuK-Architektur eine **automatische serverseitige Bereitstellungsbestätigung** vorgesehen ist. Nach der aktuellen Konzeption soll ein Application-Service (Quittungsdienst) als Erweiterung des Matrix-Homeservers automatisch bei Nachrichteneingang signierte Bereitstellungsbestätigungen erzeugen, die den Kommunikationsteilnehmern im Raum unverschlüsselt bereitgestellt werden. Diese bestehen aus vier Elementen: dem Eingangszeitpunkt im Postfach des Empfängers, einem kryptografischen Hash über das Chiffrat der Nachricht, einer Referenz auf die Originalnachricht sowie einer Signatur des empfangenden Servers, deren öffentlicher Schlüssel im Self-Service-Portal hinterlegt ist. Ist der Empfänger-Homeserver nicht erreichbar, kann eine solche Bereitstellungsbestätigung nicht erzeugt werden (ADR-0018, Abschnitt 5.4.12 und 5.5.4 des Konzepts). Die absendende Behörde kann insofern direkt überprüfen, ob und zu welchem Zeitpunkt die Nachricht das Empfänger-Backend erreicht hat. Dies schließt den Absendungsvorgang logisch mit ein. Zur Beweiskraft einer Bereitstellungsbestätigung siehe D.VI.2.2.

- Werden **Anhänge** nicht gemeinsam mit der Nachricht über das Matrix-Protokoll in das Empfänger-Backend übertragen (**Push-Prinzip**), sondern verbleiben diese zunächst physisch im Media-Repository des Absender-Servers und können vom Empfänger lediglich über einen mit der Nachricht übermittelten Link abgerufen werden (**Pull-Prinzip**), liegt diesbezüglich kein elektronischer Übermittlungsvorgang im Sinne der §§ 41 Abs. 2 VwVfG, 37 Abs. 2 SGB X oder 122 Abs. 2a AO vor. Solange sich die Datei ausschließlich auf dem Backend des Absenders befindet, kann nicht von einem Zugang und daher auch nicht von einer Bekanntgabe des Anhangs im Sinne der

genannten Vorschriften ausgegangen werden. Insofern sind die Ausführungen zum Abruf-/Bereitstellungsmodell zu berücksichtigen (siehe 2.2.2).

- Eine andere Beurteilung erscheint für den Fall eines **proaktiven Pulls** von Anhängen geboten (ADR-1120). Ruft das dezentrale Empfänger-Backend die Datei unmittelbar nach Eingang der den Link enthaltenden Nachricht automatisiert vom Absender-Backend ab, spricht Überwiegendes dafür, diesen Vorgang rechtlich als elektronische Übermittlung anzusehen. Denn der Anhang gelangt in diesem Fall ohne ein Zutun des Empfängers in dessen Machtbereich. Im Falle eines proaktiven Pulls ist für den Nachweis des Zugangs ebenfalls eine automatische serverseitige Bereitstellungsbestätigung erforderlich, die den Eingang des Anhangs auf dem dezentralen Empfänger-Backend quittiert.

- Die Bereitstellungsbestätigung belegt den Eingang einer Nachricht (ggf. auch eines proaktiv durch das Empfänger-Backend abgerufenen Anhangs (s.o.)), nicht jedoch deren Entschlüsselbarkeit und Lesbarkeit durch den Empfänger. Um das Risiko einer unwirksamen Bekanntgabe und die damit verbundene Fristen- und Bestandskraftunsicherheit zu reduzieren, ist es empfehlenswert, die Infrastruktur so auszugestalten, dass Verschlüsselungsfehler entweder verhindert oder revisionssicher dokumentiert werden (siehe hierzu D.VII.1).

- Das in den §§ 122 Abs. 2a i.V.m. 87a Abs. 7 AO ausdrücklich aufgestellte Erfordernis eines **sicheren Verfahrens**, das die übermittelnde Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet, kann – wie im Gesetz ausdrücklich klargestellt wird – durch die behördenseitige Verwendung einer qualifizierten elektronischen Signatur und den Einsatz eines geeigneten Verfahrens zur Verschlüsselung erfüllt werden. Aus dem Gesetz lässt sich nicht ableiten, dass die Erzeugung einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels dafür Bestandteil der Systemfunktionalität sein muss. Daher genügt es nach Maßgabe der genannten Bestimmungen, wenn das System den unveränderten Transport der durch den jeweiligen Absender zuvor

eigenverantwortlich signierten oder gesiegelten Dokumente als Dateianhänge ermöglicht (vgl. ADR-0017, Abschnitt 5.4.12 und 5.5.4 des Konzepts). Hinsichtlich der konkreten Anforderungen an die Integrität und Vertraulichkeit und den hieraus abzuleitenden Folgerungen für ZaPuK wird auf die datenschutzrechtlichen Ausführungen unter Abschnitt D.III.3.6 verwiesen.

2.2.2. Abruf über öffentlich zugängliche Netze/Bereitstellung zum (Daten-)Abruf – zentraler Backend-Betrieb

Kurzzusammenfassung: Erfolgt die Bekanntgabe über ein zentral, durch staatliche Stellen bereitgestelltes Empfänger-Backend, spricht vieles für die Heranziehung der Vorschriften über die Bekanntgabe durch Bereitstellung zum (Daten-)Abruf bzw. den Abruf über öffentlich zugängliche Netze (§ 9 OZG, § 122a AO, § 37 Abs. 2a und 2b SGB X, ggf. § 41 Abs. 2a VwVfG).

Die digitale Bekanntgabe setzt grundsätzlich eine Einwilligung des Adressaten voraus. In § 9 OZG ist diesbezüglich eine Fiktionslösung vorgesehen; in § 122a AO nunmehr eine Widerspruchslösung. Eine Grundlage für eine allgemeine, einwilligungslose proaktive Adressierung von Privatpersonen über einen elektronischen Kommunikationskanal wird hierdurch allerdings nicht geschaffen (vgl. die Ausführungen zur proaktiven Kommunikation unter D.II.1). Der Datenabruf setzt zudem die Authentisierung/Authentifizierung der abrufberechtigten Person voraus. Die in der ZaPuK-Architektur vorgesehenen Systeme für die Authentifizierung und die Ausstellung der Identitätsnachweise folgen im Wesentlichen den bestehenden und absehbaren gesetzlichen Lösungen. Für das ZaPuK-Postfach empfiehlt es sich, die zulässigen Mittel für die Identifizierung und Authentifizierung nach dem Vorbild der in Art. 2 des Gesetzentwurfs der Bundesregierung zum Digitale Identitätengesetz vorgesehenen Neufassung des § 3 OZG gesetzlich ausdrücklich zu regeln. Der elektronische Verwaltungsakt muss zudem speicherbar sein. Eine niederschwellige Export-/Download-Funktion ist daher zwingend vorzusehen.

Aus den verschiedenen Bekanntgaberegelungen ergeben sich für das Vorhaben nach der bisherigen Gesetzeslage unterschiedliche Anforderungen an die zu berücksichtigenden Systemfunktionen:

§ 41 Abs. 2a VwVfG ermöglicht die Bekanntgabe eines elektronischen Verwaltungsakts durch Abruf über öffentlich zugängliche Netze. Die Vorschrift gilt grundsätzlich technologieneutral, wird jedoch durch § 9 Abs. 1 OZG verdrängt, soweit die Bekanntgabe über OZG-Nutzerkonten erfolgt. Für eine vom OZG-Nutzerkonto entkoppelte Postfacharchitektur käme § 41 Abs. 2a VwVfG zur Anwendung, sofern eine Anpassung des § 9 OZG nicht erfolgt. Die Vorschrift setzt einen tatsächlichen Abruf voraus; lediglich der Zeitpunkt der Bekanntgabe wird auf den Tag nach dem Abruf fingiert. Für ZaPuK würde die Anwendbarkeit von § 41 Abs. 2a VwVfG bedeuten, dass das System zwingend den Abruf des in der Nachricht oder im Anhang enthaltenen Verwaltungsakts erfassen müsste.

§ 9 Abs. 1 OZG regelt dagegen die Bekanntgabe über das Postfach eines OZG-Nutzerkontos. Zwar knüpft die Vorschrift formal an den Abruf des Verwaltungsakts an, tatsächlich erfolgt die Bekanntgabe jedoch über eine gesetzliche Fiktion: Der Verwaltungsakt gilt am vierten Tag nach der Bereitstellung zum Abruf als bekannt gegeben. Die Behörde muss im Zweifel die Bereitstellung und deren Zeitpunkt nachweisen. Die Benachrichtigung über die Bereitstellung dient dabei lediglich der Information des Nutzers. Soll § 9 OZG ungeachtet des jeweiligen Betriebsmodells (zentral oder dezentral) auf die ZaPuK-Postfächer Anwendung finden, müsste die Regelung so angepasst werden, dass sie einheitlich an die qualifizierte Abrufumgebung der ZaPuK-Infrastruktur anknüpft. Für eine rechtssichere Bekanntgabe nach § 9 OZG müsste das System den Vorgang der Bereitstellung und dessen Zeitpunkt nachweisen können.

§ 122a AO regelt die Bekanntgabe im Steuerverwaltungsverfahrensrecht durch Bereitstellung zum Datenabruf und stellt unmittelbar auf die Bereitstellung als Bekanntgabeakt ab. Der Verwaltungsakt gilt am vierten Tag nach der Bereitstellung als bekannt gegeben. Maßgeblich ist im Zweifel der nachweisbare Zeitpunkt der Bereitstellung. Diese muss über ein sicheres Verfahren nach § 87a Abs. 8 AO erfolgen, das die für die Datenbereitstellung verantwortliche Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet. Die Regelungen aus § 122a Abs. 1 bis 4 AO finden gemäß § 122a Abs. 5 AO auch dann Anwendung, wenn die Finanzbehörde den Verwaltungsakt „im Postfach des Nutzerkontos nach dem Onlinezugangsgesetz“ zum Abruf bereitstellen will. Die Bekanntgabe von Steuerverwaltungsakten ist also nicht auf eigene Verfahren der Finanzverwaltung

beschränkt. Der Wortlaut von § 122a Abs. 5 AO sollte jedoch entsprechend auf ZaPuK angepasst werden (Entkoppelung des Postfachs vom Nutzerkonto).

§ 37 Abs. 2a SGB X regelt die Bekanntgabe im Sozialverwaltungsverfahrensrecht durch Bereitstellung zum Datenabruf. Anders als die OZG- oder die AO-Regelung knüpft die Bestimmung hinsichtlich der Bekanntgabefiktion an die Absendung der Benachrichtigung über die Bereitstellung an; im Zweifel hat die Behörde *deren* Zugang nachzuweisen. Kann sie das nicht, ist auf den Abruf abzustellen. Ausweislich der Gesetzesbegründung zu § 37 Abs. 2a SGB X handelt es sich bei der Vorschrift im Verhältnis zu § 9 OZG um die speziellere Regelung. Die Bekanntgabe eines Verwaltungsakts aus dem Bereich der Sozialverwaltung über ein ZaPuK-Postfach würde danach die Einhaltung der in § 37 Abs. 2a SGB normierten Anforderungen voraussetzen. Über die Einhaltung des Einwilligungserfordernisses hinaus würde dies für eine rechtssichere Bekanntgabe über ZaPuK in erster Linie bedeuten, dass im Zweifelsfall der Zugang der elektronischen Benachrichtigung nachweisbar sein müsste. Ist dies nicht möglich, muss der Abruf durch das System erfassbar sein.

In Angelegenheiten nach dem Abschnitt 1 des Bundeselterngeld- und Elternzeitgesetzes wird nach § 37 Abs. 2b SGB X dagegen vollständig auf die Regelung in § 9 OZG verwiesen.

Erfolgt eine Bekanntgabe über die zentral – durch staatliche Stellen und nach Stakeholdergruppen separiert – betriebenen Empfänger-Backends der ZaPuK-Infrastruktur spricht einiges dafür, die Bestimmungen über die Bekanntgabe durch Bereitstellung zum (Daten-)Abruf bzw. des Abrufs über öffentlich zugängliche Netze aus § 41 Abs. 2a VwVfG bzw. § 9 Abs. 1 OZG und den §§ 122a AO sowie 37 Abs. 2a und Abs. 2b SGB X heranzuziehen.

Die gesetzlichen Vorschriften über die Portal-/Postfachbekanntgabe folgen keinem einheitlichen Regelungskonzept. Die einzelnen Bestimmungen weisen hinsichtlich ihrer Tatbestandsvoraussetzungen und ihrer Rechtsfolgen zum Teil deutliche Unterschiede auf.[201]

[201] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 102q.

a) Einwilligungserfordernis, Authentisierung/Authentifizierung, Speicherbarkeit

Vergleichbare Anforderungen bestehen – zumindest überwiegend – hinsichtlich der geforderten Einwilligung der Adressaten in die Bereitstellung, der Authentisierung/Authentifizierung der abrufberechtigten Person und der Speicherbarkeit des bereitgestellten Verwaltungsakts.

aa) Einwilligung

Die digitale Bekanntgabe eines Verwaltungsakts durch Abruf über öffentlich zugängliche Netze bzw. durch Bereitstellung zum (Daten-)Abruf setzt nach § 41 Abs. 2a Satz 1 VwVfG, § 37 Abs. 2a Satz 1 SGB X und § 9 Abs. 1 OZG grundsätzlich die Einwilligung der jeweiligen Adressaten voraus.

Dies wird in den Gesetzesmaterialien zu § 9 Abs. 1 OZG damit begründet, dass die Verwaltungsakte nicht wie bei der herkömmlichen Bekanntgabe von der Behörde an den Adressaten zugesendet, sondern nur zum Abruf (in dem elektronischen Postfach des Nutzerkontos) bereitgestellt werden. Diese Form der Bekanntgabe erfordere für die tatsächliche Kenntnisnahme des Verwaltungsakts das Zutun des Adressaten und könne von der Behörde daher nur mit Einwilligung des Betroffenen gewählt werden. Das setze grundsätzlich voraus, dass die Behörde bei der Einholung der Einwilligung über die Besonderheiten dieser Form der Bekanntgabe informiere. Mit der Einwilligung übernehme der Beteiligte die Obliegenheit, das Postfach in diesem Sinne – wie den eigenen Briefkasten oder das E-Mail-Postfach bei der herkömmlichen Versendung – zu kontrollieren.[202]

Die OZG-Regelung bedient sich zwar seit Beginn des Jahres 2025 in **§ 9 Abs. 1 Satz 2 OZG** einer **Fiktionslösung**. Nach dieser gilt die Einwilligung als erteilt, sofern der Nutzer nicht im Rahmen der Inanspruchnahme einer elektronischen Verwaltungsleistung eine elektronische Bekanntgabe über ein Postfach im Sinne des § 2 Abs. 7 OZG ausschließt. Die Fiktionslösung knüpft aber ihrem Wortlaut nach noch immer an die vorherige Inanspruchnahme einer

[202] Begründung zu § 9 Abs. 1 OZG, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 20 f.

elektronischen Verwaltungsleistung durch den Nutzer an (vgl. hierzu auch die Ausführungen zur proaktiven Kontaktaufnahme durch die Behörde unter D.II.1.).

Im Kontext des **§ 122a AO** wird nunmehr auf die Notwendigkeit einer Einwilligung des Empfängers verzichtet. Diese findet im Gesetz seit Beginn des Jahres 2026 keine Erwähnung mehr. Stattdessen gilt dort nun eine **Widerspruchslösung**, nach der eine Bereitstellung zum Datenabruf dann ausscheidet, wenn der Beteiligte eine einmalige oder dauerhafte postalische Bekanntgabe nach § 122 Abs. 2 AO beantragt hat (§ 122a Abs. 2 Satz 1 AO). Diese Regelung ist allerdings im Zusammenhang mit § 122a Abs. 1 Satz 2 AO zu betrachten. Die Vorschrift enthält eine ermessenslenkende Regelung, nach der mittels Bereitstellung insbesondere bekannt gegeben werden soll, wenn ein Steuerbescheid, Steuermessbescheid oder Feststellungsbescheid auf einer nach § 87a Abs. 6 AO elektronisch übermittelten Steuererklärung oder Feststellungserklärung beruht und sie entweder vom Beteiligten selbst über ein von der Finanzverwaltung bereitgestelltes Nutzerkonto (§ 122a Abs. 1 Satz 2 Nr. 1 AO) oder durch eine Person im Sinne des § 80 Abs. 2 AO (insbesondere Steuerberater und Rechtsanwälte) übermittelt wurde, der gegenüber der Bescheid nach § 122 Abs. 1 Satz 4 AO bekanntzugeben ist (§ 122a Abs. 1 Satz 2 Nr. 2 AO). Die Regelung ist gemäß § 28 Abs. 2 Satz 2 Einführungsgesetz zur Abgabenordnung erstmalig auf Verwaltungsakte anzuwenden, die nach dem 31. Dezember 2026 erlassen worden sind. Praktische Relevanz habe die Widerspruchsregelung nach der Gesetzesbegründung also insbesondere in den Fällen, in denen die genannten Bescheide auf einer im Verfahren ELSTER oder einem anderen sicheren Verfahren nach § 87a Abs. 6 AO elektronisch übermittelten Steuer- oder Feststellungserklärung beruhe. Sei die Steuer- oder Feststellungserklärung dagegen zulässigerweise „auf Papier" abgegeben worden, solle die Bekanntgabe des Bescheids grundsätzlich postalisch erfolgen.[203]

Eine Grundlage für eine allgemeine, einwilligungslose proaktive Adressierung von Privatpersonen über einen elektronischen Kommunikationskanal wird auch durch die Regelungen in § 9

[203] Begründung zu § 122a AO, Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 20/11306 – Entwurf eines Vierten Gesetzes zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (Viertes Bürokratieentlastungsgesetz) vom 25.09.2024, Drucksache 20/13015, S. 101.

OZG und § 122a AO nicht geschaffen (vgl. die Ausführungen zur proaktiven Kommunikation unter D.II.1.).

bb) Authentisierung/Authentifizierung der abrufberechtigten Person

Die Bestimmungen in § 41 Abs. 2a Satz 2 VwVfG, § 9 Abs. 1 Satz 3 OZG und § 37 Abs. 2a Satz 3 SGB X sehen jeweils vor, dass die Behörde zu gewährleisten hat, dass der Abruf nur nach Authentifizierung der berechtigten Person möglich ist. Auch im Bereich der Steuerverwaltung ist in § 122a Abs. 3 AO vorgesehen, dass sich die für den Datenabruf berechtigte Person zu authentisieren hat – dort konkret nach Maßgabe des § 87a Abs. 8 AO.

(1) Bisherige Regelung im OZG

Im OZG-Regelungsregime wird der Abruf des Verwaltungsakts nach aktueller Gesetzeslage an das Nutzerkonto gekoppelt. Das „Nutzerkonto" wird in § 2 Abs. 5 Satz 1 OZG als eine zentrale IT-Komponente **zur einmaligen oder dauerhaften Identifizierung und Authentifizierung der Nutzer zu Zwecken der** Inanspruchnahme von Verwaltungsleistungen der öffentlichen Verwaltung sowie zur **vorgangsbezogenen sicheren Kommunikation über ein Postfach im Sinne des § 2 Abs. 7 OZG** definiert. Ein Nutzerkonto wird als Bürger- oder Organisationskonto bereitgestellt (§ 2 Abs. 5 Satz 2 OZG).

Konkrete Regelungen zur Identifizierung und Authentifizierung im Nutzerkonto finden sich in § 3 OZG. Für natürliche Personen (Nutzer im Sinne des § 2 Abs. 4 Nr. 1 OZG) ist dort vorgesehen, dass die Identifizierung und Authentifizierung für die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund über das zentrale Bürgerkonto des Bundes erfolgt, soweit durch Bundesgesetz keine andere Bestimmung getroffen wird (§ 3 Abs. 1 Satz 1 OZG).

§ 3 Abs. 4 OZG enthält sodann eine enumerative Aufzählung der Mittel zum Identitätsnachweis im Bürger- und Organisationskonto:[204] Für elektronische Verwaltungsleistungen, für die höchstens das Vertrauensniveau „substantiell" erforderlich ist, erfolgt der Nachweis der Identität des

[204] Begründung zu § 3 OZG, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 23.08.2023, Drucksache 20/8093, S. 39.

Nutzers nach § 3 Abs. 4 Nr. 1 lit. a und Nr. 2 OZG sowohl im Bürgerkonto als auch im einheitlichen Organisationskonto durch ein sicheres Verfahren nach § 87a Abs. 6 AO oder durch ein anderes nach Art. 6 eIDAS-VO mindestens mit dem Sicherheitsniveau „substantiell" (Art. 8 Abs. 2 lit. b der eIDAS-VO) anerkanntes elektronisches Identifizierungsmittel (§ 3 Abs. 4 Nr. 1 lit. a und Nr. 2 OZG). Für elektronische Verwaltungsleistungen, für die das Vertrauensniveau „hoch" erforderlich ist, erfolgt der Nachweis der Identität des Nutzers im Bürgerkonto durch einen elektronischen Identitätsnachweis (§ 18 Personalausweisgesetz (PAuswG), § 12 eID-Karte-Gesetz (eIDKG) oder § 78 Abs. 5 Aufenthaltsgesetz (AufenthG)) oder durch ein anderes nach Art. 6 der eIDAS-VO mit dem Sicherheitsniveau „hoch" (Art. 8 Abs. 2 lit. c der eIDAS-VO) anerkanntes elektronisches Identifizierungsmittel (§ 3 Abs. 4 Nr. 1 lit. b OZG). Die unterschiedlichen Anforderungen an das Sicherheitsniveau von Bürgerkonto und einheitlichem Organisationskonto erklärt der Gesetzgeber in den Gesetzesmaterialien mit der zum Zeitpunkt des Inkrafttretens der Regelung fehlenden Verfügbarkeit von Identifizierungsmitteln auf dem Sicherheitsniveau „hoch" für Unternehmen. Für das Bürgerkonto hatte der Gesetzgeber im Wesentlichen den Einsatz des Online-Ausweises vor Augen. Nach der eIDAS-VO anerkannte Mittel sollten demgegenüber die grenzüberschreitende Identifizierung und Authentifizierung von EU-Bürgern ermöglichen. Für das Organisationskonto ging der Gesetzgeber vorerst von der Nutzung des ELSTER-Softwarezertifikats (als sicheres Verfahren nach § 87a Abs. 6 Satz 1 AO) aus.[205]

(2) Gesetzesentwurf zum Digitale Identitätengesetz

In diesem Zusammenhang ist auch der aktuelle Gesetzentwurf der Bundesregierung zum Digitale Identitätengesetz (DIdG-E) zu berücksichtigen.[206]

Mit Art. 2 DIdG-E sollen § 3 Abs. 1 Satz 1 OZG und § 3 Abs. 4 und 5 OZG neu gefasst werden.

[205] Begründung zu § 3 OZG, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 23.08.2023, Drucksache 20/8093, S. 40.

[206] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG) vom 29.07.2026, Drucksache 21/7408.

Für die Identifizierung und Authentifizierung von natürlichen Personen für die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund treten nach der Entwurfsfassung des neuen § 3 Abs. 1 Satz 1 OZG – soweit ein Bundesgesetz nicht etwas anderes regelt – neben das zentrale Bürgerkonto des Bundes der elektronische Identitätsnachweis (bzw. ein anderes nach der eIDAS-VO mindestens mit dem Sicherheitsniveau „hoch" anerkanntes elektronisches Identifizierungsmittel) und die Europäische Brieftasche für die Digitale Identität (Art. 3 Nr. 42 der Verordnung (EU) Nr. 910/2014). Die Europäische Brieftasche für die Digitale Identität soll zudem als Nachweismittel für die Identität des Nutzers sowohl im Bürgerkonto als auch im einheitlichen Organisationskonto für die Vertrauensniveaus „substantiell" und „hoch" zu den bisherigen Nachweismöglichkeiten hinzutreten (Entwurfsfassung des neuen § 3 Abs. 4 OZG).

Ausweislich der Gesetzesbegründung soll die Änderung klarstellen, dass die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund künftig auch ohne Nutzerkonto unmittelbar über den elektronischen Identitätsnachweis oder über eine Europäische Brieftasche für die Digitale Identität erfolgen könne; Bürgerinnen und Bürger sowie Unternehmen Verwaltungsleistungen also auch ohne freiwilliges Nutzerkonto entsprechend in Anspruch nehmen könnten.[207]

(3) Regelung im Bereich der Steuerverwaltung

Für den Bereich der **Steuerverwaltung** ordnet § 87a Abs. 8 AO – auf den § 122a Abs. 3 AO verweist – zum einen an, dass ein sicheres Verfahren zu verwenden ist, welches die für die Datenbereitstellung verantwortliche Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet (Satz 1) und zum anderen, dass sich die abrufberechtigte Person zu authentisieren hat (Satz 2). Wird zur Authentisierung der elektronische Identitätsnachweis (nach § 18 PAuswG, § 12 eIDKG oder § 78 Abs. 5

[207] Begründung zu Art. 2 DIdG-E, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG) vom 29.07.2026, Drucksache 21/7408, S. 84.

AufenthG) genutzt, dürfen die dazu erforderlichen Daten zusammen mit den übrigen übermittelten Daten gespeichert und verwendet werden (§§ 87a Abs. 6 Satz 2 und Abs. 8 Satz 3 AO).

(4) Folgerungen für die ZaPuK-Architektur

- Die in der ZaPuK-Architektur vorgesehenen Systeme für die Authentifizierung und die Ausstellung der Identitätsnachweise folgen danach grundsätzlich den bestehenden und absehbaren gesetzlichen Lösungen. Für Privatpersonen sollen Lösungen wie BundID, eID und perspektivisch auch die EUDI-Wallet eingesetzt werden; für Organisationen soll die Authentifizierung über das Organisationskonto („Mein Unternehmenskonto") und perspektivisch die European Business Wallet erfolgen (ADR-0014 bis ADR-0016, Einleitung und Abschnitt 5.4.5. des Konzepts).

- Für das ZaPuK-Postfach empfiehlt es sich, die zulässigen Mittel für die Identifizierung und Authentifizierung nach dem Vorbild der in Art. 2 DIdG-E vorgesehenen Neufassung des § 3 OZG gesetzlich ausdrücklich zu regeln. Sofern das ZaPuK-Postfach direkt im OZG verankert werden soll, ist zu empfehlen, § 3 OZG um einen entsprechenden Absatz für das ZaPuK-Postfach zu ergänzen.

cc) Speicherbarkeit des Verwaltungsakts

Gemäß § 41 Abs. 2a Satz 2 VwVfG, § 9 Abs. 1 Satz 3 OZG und § 37 Abs. 2a Satz 3 SGB X hat die Behörde ferner zu gewährleisten, dass der elektronische Verwaltungsakt vom Adressaten gespeichert werden kann. Ein System mit reiner Lesefunktion würde dieser Anforderung nicht genügen.[208]

Für ZaPuK bedeutet das, dass Nutzer abgerufene Dokumente selbst speichern/exportieren können müssen. Eine niedrigschwellige Export-/Download-Funktion sollte daher zwingend vorgesehen werden.

[208] Begründung zu § 41 Abs. 2a VwVfG des Bundes, Beschlussempfehlung und Bericht des Finanzausschusses (7. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/7457 – vom 11.5.2016, Drucksache 18/8434, S. 123.

b) Bekanntgabe/-fiktionen nach den jeweiligen Vorschriften

aa) Bekanntgabe nach § 41 Abs. 2a VwVfG

Nach der allgemeinen verwaltungsverfahrensrechtlichen Regelung des § 41 Abs. 2a VwVfG des Bundes kann ein elektronischer Verwaltungsakt mit Einwilligung des Beteiligten dadurch bekannt gegeben werden, dass er vom Beteiligten oder von seinem Bevollmächtigten über öffentlich zugängliche Netze abgerufen wird. Die Behörde kann den bekanntzugebenden Verwaltungsakt also beispielsweise auf einer Internetplattform zum Abruf bereitstellen, von der der Adressat den Verwaltungsakt jederzeit und ortsunabhängig über das Internet abrufen kann.[209] Die Vorschrift ist nicht auf eine bestimmte Netz- oder Technologieform beschränkt.[210] Sie wird aber insoweit verdrängt, als die Bekanntgabe gerade über Postfächer der OZG-Nutzerkonten erfolgt.[211] Die Anwendbarkeit der in § 9 Abs. 1 OZG enthaltenen Regelung auf ZaPuK würde eine entsprechende Anpassung der Vorschrift erfordern, durch die dessen Anwendungsbereich auf eine vom Nutzerkonto entkoppelte Postfacharchitektur erstreckt wird. Erfolgt eine derartige Anpassung nicht, gelten für ZaPuK die Ausführungen zu § 41 Abs. 2a VwVfG.

Die Bekanntgabe wird nach § 41 Abs. 2a Satz 3 VwVfG für den Tag nach dem Abruf fingiert („*gilt am Tag nach dem Abruf als bekannt gegeben*"). Unter „Abruf" ist dabei das Aufrufen und Öffnen der bereitgestellten Datei zum Zweck der Kenntnisnahme zu verstehen. Regelmäßig erfolgt dies durch Anklicken der Datei.[212] Die zeitliche Festlegung der Fiktionswirkung soll dem Umstand Rechnung tragen, dass ein Abruf bis zum Ende eines Kalendertages erfolgen kann.[213] Die Fiktion soll insofern eine Gleichbehandlung der „Abrufenden" gewährleisten, unabhängig davon, zu welcher Tageszeit der Abruf erfolgt.[214] Der erstmalige Abruf selbst wird nicht fingiert,

---

[209] Begründung zu § 41 Abs. 2a VwVfG des Bundes, Beschlussempfehlung und Bericht des Finanzausschusses (7. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/7457 – vom 11.5.2016, Drucksache 18/8434, S. 122.

[210] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 105.

[211] Schulz, OZG 2.0: Ein weiterer Schritt zum vollständig digitalen Verwaltungsverfahren, NVwZ 2024, 1703 (1707).

[212] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 111.

[213] Ebd., Rn. 124.

[214] U. Stelkens, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 41, Rn. 134s.

sondern muss tatsächlich erfolgt sein. Er bildet die tatbestandliche Voraussetzung für den Eintritt der Bekanntgabefiktion.[215] Für die Feststellung des Eintritts der Fiktionswirkung ist es daher erforderlich, dass der erstmalige Abruf durch die Behörde technisch erfasst und protokolliert wird.[216] Die Anknüpfung der wirksamen Bekanntgabe an den tatsächlichen Abruf sei nach der Gesetzesbegründung besonders bürgerfreundlich und fördere die Akzeptanz der auf Freiwilligkeit beruhenden Bekanntgabeform.[217]

Zwar enthält § 41 Abs. 2a VwVfG keine ausdrückliche Verpflichtung der Behörde, den Beteiligten über die Bereitstellung zu informieren. Aus § 41 Abs. 2a Satz 4 VwVfG ergibt sich jedoch, dass der Gesetzgeber eine entsprechende Benachrichtigung voraussetzt.[218] Nach § 41 Abs. 2a Satz 4 VwVfG wird die Bereitstellung beendet, wenn der Verwaltungsakt nicht innerhalb von zehn Tagen nach Absendung einer Benachrichtigung über die Bereitstellung abgerufen wird. Die Bekanntgabe ist in diesem Fall nicht bewirkt und muss durch eine neue Bereitstellung oder anderweitige Bekanntgabe erneut vorgenommen werden (vgl. § 41 Abs. 2a Satz 5 VwVfG). Bei der Benachrichtigung handelt es sich weder um einen eigenen Verwaltungsakt noch um eine rechtsverbindliche Zusage. Ihre Ausgestaltung steht im Ermessen der Behörde.[219]

Für ZaPuK würde die Anwendbarkeit von § 41 Abs. 2a VwVfG bedeuten, dass das System für eine rechtssichere Bekanntgabe zwingend den Abruf des in der Nachricht oder im Anhang enthaltenen Verwaltungsakts erfassen müsste.

[215] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 124.
[216] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 124; U. Stelkens, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 41, Rn. 134s.
[217] Begründung zu § 41 Abs. 2a VwVfG des Bundes, Beschlussempfehlung und Bericht des Finanzausschusses (7. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/7457 – vom 11.5.2016, Drucksache 18/8434, S. 123.
[218] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 118.
[219] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 118.

bb) Bekanntgabe nach § 9 Abs. 1 OZG

§ 9 Abs. 1 OZG regelt nach derzeitiger Fassung speziell die Bekanntgabe über ein Postfach eines OZG-Nutzerkontos im Sinne des § 2 Abs. 7 OZG.

Gemäß § 9 Abs. 1 Satz 1 OZG kann ein elektronischer Verwaltungsakt mit Einwilligung des Nutzers dadurch bekannt gegeben werden, dass er vom Nutzer oder seinem Bevollmächtigten über öffentlich zugängliche Netze von dessen Postfach nach § 2 Abs. 7 OZG[220]**,** das Bestandteil eines Nutzerkontos nach § 2 Abs. 5 OZG ist, abgerufen wird. Zu der in § 9 Abs. 1 Satz 2 OZG enthaltenen Fiktion der Einwilligung siehe D.II.2.2.2.a)aa).

Die Vorschrift stellt zwar formal auf den tatsächlichen „Abruf" als Bekanntgabeakt ab, fingiert den Bekanntgabeakt allerdings unwiderleglich in § 9 Abs. 1 Satz 4 OZG und knüpft diese Fiktion an die Bereitstellung.[221] Der Verwaltungsakt gilt nach § 9 Abs. 1 Satz 4 OZG **am vierten Tag nach der Bereitstellung zum Abruf** als bekannt gegeben. Im Zweifel hat die Behörde für den Eintritt der Fiktionswirkung die **Bereitstellung und den Zeitpunkt der Bereitstellung nachzuweisen** (§ 9 Abs. 1 Satz 5 OZG).

In den Gesetzesmaterialien wird die **Zugangsfiktion** wie folgt begründet:

> *„Da die Erfassung und Protokollierung des tatsächlichen Abrufs und damit eine beweissichere Feststellung des tatsächlichen Zugangs durch die am Portalverbund beteiligten Behörden gegenwärtig technisch zu aufwändig und auf absehbare Zeit nicht durchgängig gewährleistet ist, wird der Zugang – in Anlehnung an die Regeln zur Bekanntgabe durch Versendung – fingiert. Maßgeblich für die Zugangsfiktion ist die Bereitstellung zum Abruf, über die der Betroffene benachrichtigt wird. Sie tritt an die Stelle der Versendung bei der herkömmlichen Bekanntgabe. […] Die Bereitstellung wird dokumentiert und lässt sich im*

[220] § 2 Abs. 7 Satz 1 OZG definiert das „Postfach" als eine IT-Komponente, über die Nutzer medienbruchfrei, barrierefrei und sicher mit den an den Portalverbund angeschlossenen öffentlichen Stellen vorgangsbezogen kommunizieren können sowie elektronische Dokumente und Informationen senden und empfangen können (§ 2 Abs. 7 Satz 1 OZG). Das Postfach ist Bestandteil eines Nutzerkontos (§ 2 Abs. 7 Satz 2 OZG).

[221] U. Stelkens, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Auflage 2023, § 41, Rn. 134q.

Rahmen der ordnungsgemäßen Aktenführung gerichtsfest nachweisen. Eine Anknüpfung der Zugangsfiktion an die Benachrichtigung über die erfolgte Bereitstellung zum Abruf bietet keine vergleichbare Rechtsklarheit. Denn die Behörde könnte zwar die Versendung nachweisen, nicht aber den Zugang der Benachrichtigung. […] Unter Umständen kann die gescheiterte Benachrichtigung auch erst mit erheblicher zeitlicher Verzögerung zu Tage treten. Der zur Widerlegung der Zugangsfiktion vorgetragenen Behauptung, die Benachrichtigung nicht erhalten zu haben, könnte die Behörde mangels Nachweis des Abrufs nichts entgegenhalten, selbst wenn der Beteiligte den Verwaltungsakt tatsächlich zur Kenntnis genommen hätte. Die Bereitstellung des Verwaltungsaktes durch die Behörde – zum jederzeit möglichen Abruf durch den Nutzer – im Postfach des Nutzerkontos entspricht dem Bekanntgabeakt der Versendung in der herkömmlichen Form der Bekanntgabe. […] Die Kenntnisnahme des Verwaltungsaktes, also der Zugang durch den Abruf, soll fingiert werden, da es derzeit technisch noch nicht durchgängig möglich ist, den tatsächlichen Abruf des Verwaltungsaktes zu protokollieren und an das zuständige Fachverfahren zurückzumelden. […] Gegenüber dem Beteiligten ist die Verwendung einer Fiktion in dieser Situation gerechtfertigt, weil die Bekanntgabe eines Verwaltungsaktes durch Bereitstellung zum Abruf nur durchgeführt werden kann, wenn er vorher in diese Vorgehensweise eingewilligt hat. […] Satz 4 trifft eine Beweislastregelung hinsichtlich der Bereitstellung des Verwaltungsaktes und des Zeitpunktes der Bereitstellung zu Lasten der Behörde. Die Gewährleistung der technischen Funktionsfähigkeit des Nutzerkontos liegt in der Sphäre der Behörde; dortige Unzulänglichkeiten hat sie zu vertreten. Darüber hinaus kommen Zweifel an der Möglichkeit der Kenntnisnahme durch den Beteiligten nicht in Betracht, da sich die Behörde bei der Bereitstellung eines Verwaltungsaktes im Postfach eines Nutzerkontos – anders als bei postalischer oder elektronischer

Übermittlung – nicht eines Dritten bedient. Die Verantwortungssphären von Behörde und Beteiligtem treffen unmittelbar aufeinander."[222]

Der Konzeption des § 9 Abs. 1 OZG liegt ersichtlich ein Verständnis zugrunde, nach dem der tatsächliche Zugang eines im Postfach eines OZG-Nutzerkontos bereitgestellten Verwaltungsakts – wie auch bei § 41 Abs. 2a VwVfG – grundsätzlich erst mit einer aktiven Mitwirkungshandlung des Nutzers – dem Abruf – erfolgt. Der Bereitstellungsvorgang an sich wird hingegen noch nicht als tatsächlicher Zugang gewertet, sondern stellt nur den Anknüpfungspunkt für dessen Fiktion dar. Zwar übernimmt der Nutzer mit seiner Einwilligung die Obliegenheit, das OZG-Postfach ebenso wie den eigenen Briefkasten bei der Postversendung oder das E-Mail-Postfach bei der E-Mail-Versendung zu kontrollieren. Anders als beim Briefkasten oder beim E-Mail-Postfach hat der damalige Gesetzgeber das OZG-Postfach jedoch gerade nicht als Empfangsvorrichtung angesehen, mit deren Erreichen der Verwaltungsakt bereits in den Machtbereich des Empfängers gelangt. Die Notwendigkeit der gesetzlichen Fiktion wird damit begründet, dass der tatsächliche Abruf technisch nicht beweissicher dokumentiert werden könne. Obwohl im digitalen Kontext – anders als etwa bei der postalischen Versendung – kein relevanter zeitlicher Verzug durch die Übersendung gegeben ist, auf den Rücksicht genommen werden müsste, ist der Gesetzgeber bei der Schaffung von § 9 Abs. 1 OZG ausweislich der Gesetzesbegründung davon ausgegangen, dass trotz der mit der Einwilligung übernommenen Obliegenheit zur eigenverantwortlichen Kontrolle des Postfachs noch keine gefestigte Auffassung zur Obliegenheit der täglichen Kontrolle bestand.[223]

In § 9 Abs. 1 Satz 6 OZG ist vorgesehen, dass der Nutzer oder sein Bevollmächtigter spätestens am Tag der Bereitstellung zum Abruf über die zu diesem Zweck von ihm angegebene Adresse

[222] Begründung zu § 9 Abs. 1 OZG, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 20-22.

[223] Begründung zu § 9 Abs. 1 OZG, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 21 f.

über die Möglichkeit des Abrufs benachrichtigt wird. Die Benachrichtigung hat jedoch nur eine Hinweisfunktion.[224]

Erfolgt der Abruf vor einer erneuten Bekanntgabe des Verwaltungsakts, bleibt der Tag des ersten Abrufs für den Zugang maßgeblich (§ 9 Abs. 1 Satz 7 OZG). Damit soll verhindert werden, dass in Fällen, in denen ein Abruf zunächst (z.B. aufgrund von Server-Ausfällen) nicht möglich war, eine erneut eingeleitete Bekanntgabe den Zeitpunkt der Bekanntgabe nach hinten verschiebt, obwohl zwischenzeitlich doch ein Abruf erfolgt ist. Die Regelung kommt nach den Gesetzesmaterialien nur in den Fällen zum Tragen, in denen die Behörde den tatsächlichen Abruf gerichtsfest feststellen kann.[225]

Die Anwendbarkeit des § 9 OZG auf das zentral bereitgestellte ZaPuK-Postfach würde – wie bereits dargestellt – eine Entkoppelung des Postfachbegriffs von den OZG-Nutzerkonten erfordern. Soll § 9 OZG ungeachtet des jeweiligen Betriebsmodells (zentral oder dezentral) auf die ZaPuK-Postfächer Anwendung finden, müsste die Regelung – jedenfalls ausgehend von der Gesetzesbegründung, die die mit dem Nutzerkonto verbundenen Postfächer der Sphäre der Behörde zuordnet – dabei einheitlich an die qualifizierte Abrufumgebung der ZaPuK-Infrastruktur anknüpfen. Für eine rechtssichere Bekanntgabe nach § 9 OZG müsste das System den Vorgang der Bereitstellung und dessen Zeitpunkt nachweisen können.

cc) Bekanntgabe nach § 122a AO i. V. m § 87a Abs. 8 AO

Für den Bereich des Steuerverfahrensrechts bestimmt § 122a Abs. 1 Satz 1 AO, dass Verwaltungsakte dem Beteiligten oder der von ihm bevollmächtigten Person bekannt gegeben werden können, indem sie nach § 87a Abs. 8 AO zum Datenabruf bereitgestellt werden. Die Vorschrift knüpft somit auch formal nicht mehr an den Abruf an, sondern stellt direkt auf die Bereitstellung als Bekanntgabeakt ab.

[224] Begründung zu § 9 Abs. 1 OZG, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 22.
[225] Ebd.

Wird ein elektronisch erlassener Verwaltungsakt durch Bereitstellung zum Abruf nach § 122a AO bekannt gegeben, ist nach der Bestimmung des § 87a Abs. 8 AO ein sicheres Verfahren zu verwenden, das die für die Datenbereitstellung verantwortliche Stelle oder Einrichtung der Finanzverwaltung authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet (§ 87a Abs. 8 Satz 1 AO). Die Gesetzesbegründung zu § 87a Abs. 8 AO enthält keine konkrete Beschreibung, wie das sicherere Verfahren ausgestaltet sein muss, nennt für die Authentifizierung der für die Datenbereitstellung verantwortlichen Stelle jedoch beispielhaft noch die Verwendung eines SSL-Zertifikats.[226] Gemäß Ziffer 1 des Anwendungserlasses des Bundesministeriums der Finanzen zu § 122a AO wird durch die Datenbereitstellung von Verwaltungsakten der Landesfinanzbehörden über die Kommunikationsplattform ELSTER im Format PDF/A ein sicheres Verfahren verwendet, das die Vertraulichkeit und Integrität des Datensatzes gewährleistet (§ 87a Abs. 8 AO).[227] Aus dem Gebot der Gewährleistung der Vertraulichkeit des Datensatzes sowie aus § 87a Abs. 1 Satz 4 AO folgt, dass bei der durch den Datenabruf ausgelösten Datenfernübertragung des Verwaltungsakts die Daten mit einem geeigneten Verfahren zu verschlüsseln sind. Die abrufberechtigte Person kann jedoch auf eine Verschlüsselung verzichten.[228]

§ 122a Abs. 4 Satz 1 AO enthält eine gesetzliche Bekanntgabe-Vermutung. In Anlehnung an § 9 Abs. 1 OZG gilt ein zum Abruf bereitgestellter Verwaltungsakt danach am vierten Tag nach der Bereitstellung zum Abruf als bekannt gegeben (§ 122a Abs. 4 Satz 1 AO). Im Zweifel hat die Behörde den Zeitpunkt der Bereitstellung zum Abruf nachzuweisen (§ 122a Abs. 4 Satz 2 AO). Nach der Gesetzesbegründung entspreche die Regelung in § 122a Abs. 4 Satz 1 AO im Ergebnis der postalischen Bekanntgabe von Verwaltungsakten, bei der es ausreiche, dass der Verwaltungsakt in den Machtbereich des Empfängers gelangt sei, bei der die tatsächliche

[226] Begründung zu § 87a Abs. 8 AO, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 03.02.2016, Drucksache 18/7457, S. 65.

[227] Bundesfinanzministerium, Änderung des Anwendungserlasses zur Abgabenordnung (AEAO) vom 29.01.2026, abrufbar unter https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/AO-Anwendungserlass/2026-01-29-aenderung-aeao-46-usw.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 04.08.2026).

[228] Schmidt, Digitale Bekanntgabe von Verwaltungsakten im Besteuerungsverfahren, NJW 2025, 1688, Rn. 10.

Kenntnisnahme durch den Empfänger jedoch irrelevant sei. Nichts anderes solle für die Bekanntgabe durch Bereitstellung zum Abruf gelten.[229]

Die abrufberechtigte Person ist am Tag der Bereitstellung elektronisch über die Abrufmöglichkeit und ihre Rechtswirkungen zu benachrichtigen (§ 122a Abs. 1 Satz 3 AO). Die Benachrichtigung hat dabei jedoch nur eine Hinweisfunktion und ist nicht (mehr) Anknüpfungspunkt der gesetzlichen Bekanntgaberegelung.[230] Sie muss auch nicht verschlüsselt werden (vgl. § 87a Abs. 1 Satz 6 AO). Trägt die abrufberechtigte Person unwiderlegbar vor, die Information über die Bereitstellung nach § 122a Abs. 1 Satz 3 AO nicht erhalten zu haben, und hat sie den Verwaltungsakt auch nicht aus anderem Grund abgerufen, kann ihr unter den Voraussetzungen des § 110 AO Wiedereinsetzung in den vorigen Stand gewährt werden.[231]

Die Regelungen aus § 122a Abs. 1 bis 4 AO finden gemäß § 122a Abs. 5 AO auch dann Anwendung, wenn die Finanzbehörde den Verwaltungsakt „im Postfach des Nutzerkontos nach dem Onlinezugangsgesetz" zum Abruf bereitstellen will. Hiermit wird klargestellt, dass die Bekanntgabe von Steuerverwaltungsakten durch Bereitstellung zum Datenabruf im Sinne des § 122a Abs. 1 AO nicht auf eigene Verfahren der Finanzverwaltung (z.B. das Verfahren ELSTER) beschränkt ist. Die Finanzbehörde kann zur Bekanntgabe eines Steuerverwaltungsakts durch Bereitstellung zum Datenabruf auch das Postfach des OZG-Nutzerkontos verwenden.[232] Damit kommt etwa auch eine Bereitstellung über das Bürgerkonto in Betracht. In diesem Fall bleibt

[229] Begründung zu § 122a AO, Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 20/11306 – Entwurf eines Vierten Gesetzes zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (Viertes Bürokratieentlastungsgesetz) vom 25.09.2024, Drucksache 20/13015, S. 102.

[230] Ebd., S. 101.

[231] Bundesfinanzministerium, Änderung des Anwendungserlasses zur Abgabenordnung (AEAO) vom 29.01.2026, abrufbar unter https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/AO-Anwendungserlass/2026-01-29-aenderung-aeao-46-usw.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 04.08.2026); so auch Begründung zu § 122a AO, Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 20/11306 – Entwurf eines Vierten Gesetzes zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (Viertes Bürokratieentlastungsgesetz) vom 25.09.2024, Drucksache 20/13015, S. 102.

[232] Begründung zu § 122a Abs. 5 AO, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 25.

die Bekanntgabevermutung des § 122a Abs. 4 AO unabhängig vom genutzten Postfach bestehen.[233]

Für ZaPuK bedeutet das, dass auch für eine rechtssichere Bekanntgabe von Bescheiden aus dem Bereich der Steuerverwaltung im Zweifel der Zeitpunkt der Bereitstellung nachweisbar sein muss. Der Wortlaut von § 122a Abs. 5 AO sollte entsprechend auf ZaPuK angepasst werden (Entkoppelung des Postfachs vom Nutzerkonto).

dd) Bekanntgabe nach § 37 Abs. 2a SGB X

Für den Bereich des Sozialverfahrensrechts normiert § 37 Abs. 2a Satz 1 SGB X, dass elektronische Verwaltungsakte mit Einwilligung bekannt gegeben werden können, indem sie dem Beteiligten zum Abruf über öffentlich zugängliche Netze bereitgestellt werden.

In § 37 Abs. 2a Satz 4 SGB X ist allerdings abweichend von den zuvor dargestellten Bekanntgabevorschriften geregelt, dass ein zum Abruf bereitgestellter Verwaltungsakt am vierten Tag *nach Absendung der elektronischen Benachrichtigung* über die Bereitstellung des Verwaltungsakts an die abrufberechtigte Person als bekannt gegeben gilt. Im Zweifel hat die Behörde den Zugang der Benachrichtigung nachzuweisen (§ 37 Abs. 2a Satz 5 SGB X). Kann die Behörde den von der abrufberechtigten Person bestrittenen Zugang der Benachrichtigung nicht nachweisen, gilt der Verwaltungsakt an dem Tag als bekannt gegeben, an dem die abrufberechtigte Person den Verwaltungsakt abgerufen hat (§ 37 Abs. 2a Satz 6 SGB X). Das Gleiche gilt, wenn die abrufberechtigte Person unwiderlegbar vorträgt, die Benachrichtigung nicht innerhalb von vier Tagen nach der Absendung erhalten zu haben (§ 37 Abs. 2a Satz 7 SGB X).

Die Gesetzesmaterialien erläutern hierzu Folgendes:

> *„Die bisherige Regelung des § 37 Absatz 2a SGB X, die hinsichtlich des Zeitpunktes der Bekanntgabe von elektronischen Verwaltungsakten grundsätzlich auf den tatsächlichen Abruf durch die abrufberechtigte Person abstellt, hat sich*

[233] Schmidt, Digitale Bekanntgabe von Verwaltungsakten im Besteuerungsverfahren, NJW 2025, 1688, Rn. 35.

gerade in der Sozialverwaltungspraxis mit Massenverfahren als ineffizient und wenig praktikabel erwiesen. […] Mit der Neuregelung können elektronische Verwaltungsakte mit Einwilligung der berechtigten Person über ein Abrufverfahren in Portalen mit einer Zugangsfiktion bekannt gegeben werden. Die Zugangsfiktion knüpft dabei an den Zeitpunkt des Versands der Benachrichtigung über die Bereitstellung eines Verwaltungsaktes zum Datenabruf an. […] Mit der Rechtsänderung wird nun die bisherige Regelung des Absatzes 2a durch die Regelung des Absatz 2b ersetzt und dabei auf alle Sozialleistungsträger erstreckt. Dies ist zwingend erforderlich, da neben den Krankenkassen, der Bundesagentur für Arbeit und den Trägern der Grundsicherung für Arbeitsuchende auch bei den anderen Sozialleistungsträgern das praktische Bedürfnis für die unkomplizierte und effektive Bekanntgabe von elektronischen Verwaltungsakten besteht. Mit der Rechtsänderung wird einerseits die weitere Digitalisierung von Verwaltungsprozessen ermöglicht, andererseits werden die Rechte und die Interessen der Beteiligten des Sozialverwaltungsverfahrens gewahrt. […] Aufgrund der Besonderheiten des Sozialverwaltungsverfahrens und der oftmals schutzbedürftigen Sozialleistungsempfänger ist die verfahrensrechtliche Zugangsfiktion des § 37 Absatz 2a – neu – die speziellere Regelung gegenüber der in § 9 OZG enthaltenen Regelung. Die verfahrensrechtliche Regelung des § 37 Absatz 2a findet daher auch dann Anwendung, wenn für die Bekanntgabe eines elektronischen Verwaltungsaktes durch Bereitstellung zum Datenabruf das Postfach eines OZG-Nutzerkontos verwendet wird. Damit wird sichergestellt, dass zur Bestimmung des Bekanntgabezeitpunkts von zum Datenabruf bereitgestellten Verwaltungsakten ungeachtet des verwendeten Postfachs immer die gleichen verfahrensrechtlichen Regelungen gelten. Die mit der Bekanntgabe nach § 9 OZG verknüpfte Obliegenheit der Bürgerinnen und Bürger, das Portal regelmäßig auf Eingänge zu kontrollieren (vgl. dem Hausbriefkasten) soll zunächst schwerpunktmäßig im allgemeinen Verwaltungsverfahrensrecht erprobt werden. Die Regelungen zur Bekanntgabe von elektronischen Verwaltungsakten zum Abruf mit Fiktionswirkung sollen nach der Evaluierung

des § 9 OZG noch einmal in einer Gesamtschau mit der Zielsetzung einer einheitlichen Regelung geprüft werden."[234]

(Hervorhebung hier hinzugefügt)

Eine Bekanntgabe von Verwaltungsakten aus dem Bereich der Sozialverwaltung setzt danach auch unter Einsatz eines OZG-Postfachs grundsätzlich die Einhaltung der in § 37 Abs. 2a SGB X normierten Anforderungen voraus. Neben dem Erfordernis einer Einwilligung – auf die die Fiktionslösung somit keine Anwendung finden kann – bedeutet das für eine rechtssichere Bekanntgabe über ZaPuK in erster Linie, dass die Fiktion an die Absendung der elektronischen Benachrichtigung über die Bereitstellung des Verwaltungsakts anknüpft, deren Zugang im Zweifel nachweisbar sein müsste. Ist dies nicht möglich, muss der Abruf durch das System erfassbar sein.

ee) Bekanntgabe nach § 37 Abs. 2b SGB X i. V. m. § 9 OZG

In Angelegenheiten nach dem Abschnitt 1 des Bundeselterngeld- und Elternzeitgesetzes gilt abweichend von der Regelung in § 37 Abs. 2a SGB X für die Bekanntgabe von elektronischen Verwaltungsakten die Regelung des § 9 OZG. Die jeweiligen Elterngeldstellen der Länder haben damit elektronische Verwaltungsakte über das Elterngeld nach der OZG-Regelung bekannt zu geben.[235]

Damit sollten die für die Durchführung des Ersten Abschnitts des Gesetzes zum Elterngeld und zur Elternzeit zuständigen Verwaltungsträger in die Lage versetzt werden, die neue Regelung zur Bekanntgabe von elektronischen Verwaltungsakten in § 9 OZG zu nutzen. Nach der Gesetzesbegründung können hierdurch gewonnene Erfahrungen in eine zukünftige Prüfung einfließen, ob die Regelung zur Bekanntgabe in § 9 OZG gegebenenfalls auch hinsichtlich weiterer Sozialleistungsbereiche übernommen werden soll. Dies hat insbesondere zur Folge, dass für

[234] Begründung zu § 37 Abs. 2a SGB X, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/21987, 19/22776, 19/23054 Nr. 5 – Entwurf eines Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 28.10.2020, Drucksache 19/23774, S. 25 f.

[235] Mutschler, in: beck-online.GROSSKOMMENTAR (Kasseler Kommentar), Hrsg: Rolfs/Fuchsloch (geschf.)/Körner/Krasney/Mutschler, Stand: 15.02.2026, § 37 SGB X, Rn. 42.

eine Bekanntgabe nach § 37 Abs. 2b SGB X die Bekanntgabefiktion des § 9 Abs. 1 Satz 4 OZG maßgeblich ist.[236]

Insofern kann auf die Ausführungen unter D.II.2.2.2.b)bb) verwiesen werden.

ff) Folgerungen für die Architektur von ZaPuK

- Aus den verschiedenen Bekanntgaberegelungen ergeben sich für das Vorhaben nach der bisherigen Gesetzeslage unterschiedliche Anforderungen an die zu berücksichtigenden Systemfunktionen. Da die einzelnen Verfahrensordnungen hinsichtlich der Bekanntgabefiktion zum Teil an unterschiedliche Ereignisse anknüpfen, muss das System die jeweils relevanten Vorgänge nachvollziehbar dokumentieren können. Nur dies ermöglicht den jeweiligen Nutzern, eine rechtssichere Berechnung von Rechtsbehelfsfristen.

- Das System muss zum einen die **Bereitstellung und den Zeitpunkt der Bereitstellung** nachweisen können. Dieses Erfordernis ergibt sich aus den Regelungen, die die Bekanntgabefiktion an die Bereitstellung knüpfen (vgl. § 9 Abs. 1 Satz 4 und 5 OZG (ggf. i V. m. § 37 Abs. 2b SGB X) sowie § 122a Abs. 4 Satz 1 und 2 AO). Danach ist die Architekturentscheidung zugunsten einer **automatischen serverseitigen Bereitstellungsbestätigung** (ADR-0018) ungeachtet des jeweiligen Betriebsmodells der ZaPuK-Postfächer – dezentral oder zentral – positiv zu bewerten. Zur Beweiskraft einer Bereitstellungsbestätigung siehe D.VI.2.2.

- Auch hier gilt: Die Bereitstellungsbestätigung stellt zwar einen Beleg für den Eingang einer Nachricht dar, die Entschlüsselbarkeit und die Lesbarkeit der Nachricht durch den Empfänger lassen sich damit jedoch nicht belegen. Um das Risiko einer unwirksamen Bekanntgabe und Unsicherheiten hinsichtlich des Eintritts der Fiktionswirkung zu reduzieren, sollte die Infrastruktur daher so ausgestaltet werden, dass

[236] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 102e.

Verschlüsselungsfehler entweder verhindert oder revisionssicher dokumentiert werden (siehe hierzu D.VII.1).

- Für eine rechtssichere Bekanntgabe von Verwaltungsakten aus dem Bereich der Sozialverwaltung sollte das System grundsätzlich auch den **Zugang der Benachrichtigung über die Bereitstellung** beim Empfänger nachweisen können. Dieses Erfordernis ergibt sich aus der Bestimmung in § 37 Abs. 2a Satz 4 und 5 SGB X, die ausweislich der Gesetzesbegründung auch bei einer Bekanntgabe über ein OZG-Postfach Anwendung findet. Nach der aktuellen Konzeption von ZaPuK soll das Postfach einen Benachrichtigungsdienst enthalten, der den Empfänger über den Eingang neuer Nachrichten informiert – z.B. per E-Mail (SMTP) und Push (APN/GCM) (Abschnitt 5.2.2.1 des Konzepts). Ausgehend von der Annahme, dass sich der Zugang einer solchen Benachrichtigung beim Empfänger nicht durchgängig verlässlich nachweisen lässt, muss somit der **Abruf** des Verwaltungsakts nachvollziehbar dokumentiert werden können (vgl. § 37 Abs. 2a Satz 6 und 7 SGB X).

- Der Nachweis des **Abrufs** wäre grundsätzlich auch nach § 41 Abs. 2a Satz 3 VwVfG für den Fall erforderlich, dass die Bekanntgabe nicht im Rahmen des OZG erfolgt. Da § 9 Abs. 1 OZG in seiner derzeitigen Fassung ausdrücklich die Bekanntgabe über ein Postfach eines OZG-Nutzerkontos im Sinne des § 2 Abs. 7 OZG („Postfach nach § 2 Absatz 7, das Bestandteil eines Nutzerkontos nach § 2 Absatz 5 ist“) regelt, bedürfte es einer entsprechenden Anpassung des § 9 Abs. 1 OZG, um dessen Regelungswirkung auf eine vom Nutzerkonto entkoppelte Postfacharchitektur zu erstrecken. Soll § 9 OZG unabhängig vom jeweiligen Betriebsmodell – zentral oder dezentral – auf die ZaPuK-Postfächer Anwendung finden, müsste die Regelung dabei einheitlich an die qualifizierte Abrufumgebung der ZaPuK-Infrastruktur anknüpfen.

- Aus der Formulierung des § 9 Abs. 1 Satz 1 OZG lässt sich zudem schließen, dass die Bereitstellung eines Verwaltungsakts auf dem Postfach-Backend des Empfängers erfolgen muss. Unerheblich dürfte dabei sein, ob ein den Verwaltungsakt beinhaltender Anhang unmittelbar durch einen Upload zusammen mit der Nachricht über das

Matrix-Protokoll oder durch einen proaktiven automatisierten Abruf des Empfänger-Backends (ADR-1120) dorthin gelangt. Nicht ausreichend für eine Bekanntgabe nach § 9 Abs. 1 OZG – oder eine künftige Bekanntgaberegelung, die hinsichtlich der Bereitstellung ausdrücklich an das ZaPuK-Postfach anknüpft – wäre es hingegen, wenn das betreffende Dokument lediglich im Media-Repository des Absender-Servers bereitgestellt wird und vom Empfänger erst über einen Link von dort aus abgerufen werden muss.

- Eine Funktion zur Erfassung und Bestätigung des tatsächlichen Abrufs bleibt auch dann von Bedeutung, wenn über das ZaPuK-Postfach elektronische Dokumente durch die Behörden bereitgestellt werden, die keine Verwaltungsakte darstellen. Für solche Dokumente finden die besonderen Bekanntgaberegelungen- und Fiktionen der Verwaltungsverfahrensordnungen regelmäßig keine Anwendung. Soll der tatsächliche Zugang oder die Kenntnisnahme nachgewiesen werden, kann daher allein eine dokumentierte Abrufbestätigung den erforderlichen Nachweis erbringen.

- Die genannten Fälle unterstreichen die Architekturentscheidung zugunsten einer durch den Absender gesteuerten Zustelloption (ADR-1119) und die damit einhergehende Möglichkeit des Absenders, bei Bedarf auch die Erzeugung einer **automatischen clientseitigen Abrufbestätigung** anzufordern. Der Client (Postfachzugang) des Empfängers soll dabei ohne aktive Nutzerhandlung ein verschlüsseltes Room-Event übermitteln, sobald die Nachricht entschlüsselt und angezeigt wurde (ADR-1118, Abschnitt 5.4.12 und 5.5.4 des Konzepts). Ein modifizierter oder nicht-konformer Client kann die Abrufbestätigung zwar unterdrücken, das Ausbleiben der Abrufbestätigung wäre in diesem Fall für die Behörde jedoch nachvollziehbar.

gg) Anregungen zur Harmonisierung der Bekanntgaberegelungen

Die Zersplitterung der Bekanntgabevorschriften kann aktuell zu praktischen Abgrenzungsschwierigkeiten führen. Besonders deutlich wird dies im Anwendungsbereich des § 37 SGB X. Bezieht eine abrufberechtigte Person neben dem Elterngeld weitere Sozialleistungen, können Verwaltungsakte sowohl nach § 37 Abs. 2a als auch nach Abs. 2b SGB X über ein OZG-Postfach

bekannt gegeben werden. Obwohl in beiden Fällen dieselbe Person Adressat der Bekanntgabe ist, bestimmt sich der Beginn der Rechtsbehelfsfrist nach unterschiedlichen Regelungen. Die betroffene Person muss in einem solchen Fall mit Blick auf den Beginn der Rechtsbehelfsfristen ggf. unterschiedliche Fristberechnungen vornehmen, je nachdem welcher Absatz der Vorschrift einschlägig ist. Während die Bekanntgabefiktion gemäß § 37 Abs. 2a Satz 4 SGB X am vierten Tag nach Absendung der elektronischen Benachrichtigung über die Bereitstellung eintritt, gilt der Verwaltungsakt nach § 37 Abs. 2b SGB X i. V. m § 9 Abs. 1 Satz 4 OZG am vierten Tag nach der Bereitstellung als bekannt gegeben.[237]

Vor diesem Hintergrund ist Folgendes zu empfehlen:

- Eine harmonisierte Regelung der elektronischen Bekanntgabe von Verwaltungsakten sollte hinsichtlich der Verwendung der ZaPuK-Postfächer bereichsübergreifend an ein einheitliches Bekanntgabeereignis anknüpfen. Nur so lässt sich sowohl auf Seiten der Empfänger als auch der Behörden eine einheitliche und rechtssichere Berechnung von Rechtsbehelfsfristen gewährleisten. Es erscheint zumindest fraglich, ob die in § 37 Abs. 2a Satz 4 SGB X gegenüber § 9 OZG abweichende Anknüpfung an die Benachrichtigung über die Bereitstellung tatsächlich durch die Besonderheiten des Sozialverwaltungsverfahrens gerechtfertigt ist. Dem besonderen Schutzbedürfnis der Adressaten dürfte bereits dadurch Rechnung getragen werden, dass die Nutzung des Bürgerkontos nach § 3 Abs. 1 Satz 2 OZG freiwillig ist und die Bekanntgabe durch Bereitstellung zum Abruf nach § 37 Abs. 2a Satz 1 SGB X zudem die Einwilligung des Adressaten voraussetzt. Vor diesem Hintergrund ist nicht ohne Weiteres ersichtlich, weshalb darüber hinaus gerade für das Sozialverwaltungsverfahren ein abweichendes Bekanntgabeereignis erforderlich sein soll.

- Bei der Festlegung des maßgeblichen Bekanntgabeereignisses ist ferner zu berücksichtigen, dass ein Bekanntgabeereignis, dessen Eintritt von der Mitwirkung des

[237] Couzinet, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 41, Rn. 102e und 102q.

Empfängers abhängt, diesem auch die Möglichkeit eröffnet, den Eintritt der Bekanntgabe und damit den Beginn der Rechtsbehelfsfrist hinauszuzögern oder zu verhindern.

- Zur Förderung einer kohärenten und übersichtlichen Ausgestaltung der elektronischen Bekanntgabe sollten die allgemeinen Bekanntgaberegelungen an zentraler Stelle im Verwaltungsverfahrensrecht gebündelt werden. Fachgesetzliche Regelungen sollten hierauf grundsätzlich verweisen und lediglich insoweit eigenständige Vorschriften enthalten, als bereichsspezifische Besonderheiten dies auch wirklich erfordern.

- Selbst der nachweisliche Eingang eines elektronischen Verwaltungsakts in den Machtbereich des Empfängers dürfte eine zeitliche Bekanntgabefiktion nicht zwangsläufig entbehrlich machen, da es auch insoweit Unterschiede auszugleichen gilt, die daraus resultieren, dass ein elektronischer Verwaltungsakt zu unterschiedlichen Tageszeiten bereitgestellt oder abgerufen werden kann.

2.3. Digitale Zustellung von Dokumenten

Kurzzusammenfassung: Die elektronische Zustellung richtet sich nach den Bestimmungen des § 5 VwZG. Nach aktueller Rechtslage kann ein elektronisches Dokument nach § 5 Abs. 5 VwZG elektronisch gegen Empfangsbekenntnis zugestellt werden. Die elektronische Zustellung setzt danach einen vom Empfänger eröffneten Zugang, das Anbringen einer qualifizierten elektronischen Signatur am zuzustellenden Dokument sowie dessen Schutz vor unbefugter Kenntnisnahme voraus. An einen in § 5 Abs. 4 VwZG abschließend aufgelisteten, besonders vertrauenswürdigen Adressatenkreis (z.B. Behörden, Rechtsanwälte, Steuerberater, etc.) kann die Zustellung „auf andere Weise, auch elektronisch, gegen Empfangsbekenntnis“ unter vereinfachten Bedingungen erfolgen. Hierbei muss das zuzustellende Dokument nicht zwingend qualifiziert elektronisch signiert sein. Die besondere Zustellungsmöglichkeit über De-Mail ist dagegen aus dem Gesetz gestrichen worden.

Der Nachweis der Zustellung erfordert eine aktive Mitwirkung des Empfängers in Form eines abzugebenden Empfangsbekenntnisses, das durch den Empfänger mit Datum und Unterschrift zu versehen ist. Wird das Empfangsbekenntnis elektronisch erteilt, ist es durch den Empfänger qualifiziert elektronisch zu signieren. Eine automatische Bereitstellungs- oder Abrufbestätigung genügt den Anforderungen an das Empfangsbekenntnis nicht. Eine aktive Lesebestätigung kann die erforderliche willensgetragene Mitwirkung des Empfängers abbilden, sollte ihm aber die Möglichkeit eröffnen, das maßgebliche Zustellungsdatum selbst anzugeben, da dieses vom tatsächlichen Abruf- oder Anzeigezeitpunkt abweichen kann (siehe hierzu auch D.VI.4).

Wird ein Verfahren auf Grund einer Rechtsvorschrift auf Verlangen des Empfängers in elektronischer Form abgewickelt, greift bei Ausbleiben des Empfangsbekenntnisses unter den Voraussetzungen des § 5 Abs. 7 Satz 2 VwZG eine widerlegliche Zustellungsfiktion am vierten Tag nach der Absendung des elektronischen Dokuments.

Soll ein Bescheid oder ein anderes Dokument der Behörde über ein ZaPuK-Postfach formell nach dem Verwaltungszustellungsrecht zugestellt werden – z.B. besteht eine solche Verpflichtung bei Widerspruchsbescheiden im Sinne der VwGO[238] –, sind nach aktueller Gesetzeslage die Regelungen des § 5 VwZG über die elektronische Zustellung zu beachten.

2.3.1. Zustellung gegen Empfangsbekenntnis an einen unbeschränkten Empfängerkreis

Ein elektronisches Dokument kann nach § 5 Abs. 5 Satz 1 VwZG elektronisch zugestellt werden, soweit der Empfänger hierfür einen Zugang eröffnet. Nach § 5 Abs. 5 Satz 2 VwZG muss das Dokument sogar elektronisch zugestellt werden, wenn auf Grund einer Rechtsvorschrift ein Verfahren auf Verlangen des Empfängers in elektronischer Form abgewickelt wird. Für die Übermittlung ist das Dokument gemäß § 5 Abs. 5 Satz 3 VwZG mit einer qualifizierten elektronischen Signatur zu versehen und gegen unbefugte Kenntnisnahme Dritter zu schützen.

[238] Das Widerspruchsverfahren richtet sich nach den §§ 68 ff. VwGO. Gemäß § 73 Abs. 3 Satz 1 und 2 VwGO sind Widerspruchsbescheide von Amts wegen nach den Vorschriften des VwZG zuzustellen.

Für eine wirksame elektronische Zustellung ist es nicht ausreichend, dass das zuzustellende Dokument lediglich im Machtbereich des Adressaten eingegangen ist. Der Adressat muss das zuzustellende Dokument vielmehr mit Annahmewillen „empfangen" haben. Er muss an der Zustellung mitwirken und den Willen zum Ausdruck bringen, das Dokument als zugestellt anzusehen. Zum Nachweis der Zustellung stellt § 5 Abs. 7 Satz 1 VwZG insofern auf ein mit Datum und Unterschrift versehenes Empfangsbekenntnis ab, das an die Behörde durch die Post oder elektronisch zurückzusenden ist. Wird das Empfangsbekenntnis als elektronisches Dokument erteilt, bedarf es zum Ersatz der eigenhändigen Unterschrift einer qualifizierten elektronischen Signatur im Sinne der eIDAS-VO. Eine elektronisch generierte Eingangsbestätigung genügt den Anforderungen an den Zustellungsnachweis dagegen nicht. Aus einer solchen Bestätigung lässt sich der erforderliche Annahmewille nicht herleiten.[239]

Für die Fälle des § 5 Abs. 5 Satz 2 VwZG, in denen das Verfahren auf Verlangen des Empfängers in elektronischer Form abgewickelt wird, enthält § 5 Abs. 7 Satz 2 VwZG eine Zustellungsfiktion. Danach gilt ein elektronisches Dokument am vierten Tag nach der Absendung an den vom Empfänger hierfür eröffneten Zugang als zugestellt, wenn der Behörde nicht spätestens an diesem Tag ein Empfangsbekenntnis zugeht. Bleibt das Empfangsbekenntnis aus, wird damit eine Verweigerung der Mitwirkung an der Zustellung vermutet. Diese Vermutung kann der Empfänger nach § 5 Abs. 7 Satz 3 VwZG widerlegen, trägt dabei aber die Beweislast für den Nichtzugang oder einen späteren Zugang des Dokuments.[240] Der Empfänger ist daher vor der Übermittlung über die Rechtsfolgen der Zustellungsfiktion zu belehren und über ihren Eintritt zu benachrichtigen (§ 5 Abs. 7 Satz 4 und 6 VwZG). Zum Nachweis der Zustellung ist gemäß § 5 Abs. 7 Satz 5 VwZG von der absendenden Behörde in den Akten zu vermerken, zu welchem Zeitpunkt und an welchen Zugang das Dokument gesendet wurde.

[239] Preisner, in: BeckOK OWiG, Graf, 51. Edition, Stand: 01.07.2026, § 5 VwZG, Rn. 16 und 26.
[240] Sander/Smollich, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 5 VwZG, Rn. 18.

2.3.2. Zustellung gegen Empfangsbekenntnis an besonders vertrauenswürdige Empfänger

An den in § 5 Abs. 4 VwZG abschließend aufgelisteten, besonders vertrauenswürdigen Adressatenkreis – Behörden, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, Rechtsanwälte, Patentanwälte, Notare, Steuerberater, Steuerbevollmächtigte, Wirtschaftsprüfer, vereidigte Buchprüfer, Berufsausübungsgesellschaften im Sinne der Bundesrechtsanwaltsordnung (BRAO), der Patentanwaltsordnung (PAO) und des Steuerberatungsgesetzes (StBerG), Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften – kann die Zustellung „auf andere Weise, auch elektronisch, gegen Empfangsbekenntnis" unter vereinfachten Bedingungen erfolgen – etwa per E-Mail oder bei Rechtsanwälten per besonderem elektronischen Anwaltspostfach. Die elektronische Übermittlung setzt dabei – sofern nicht anderweitig angeordnet – keine Verwendung einer qualifizierten elektronischen Signatur voraus. [241]

2.3.3. Entfallene Möglichkeit einer Zustellung per De-Mail

Daneben ist eine Zustellung nach § 5a Abs. 1 Satz 1 VwZG a.F. durch Übermittlung an das De-Mail-Postfach des Empfängers gegen Abholbestätigung nach neuer Gesetzeslage nicht mehr möglich. § 5a VwZG a.F. ist gemäß Art. 15 Abs. 3 Nr. 2 des Gesetzes für den Bürokratierückbau im Bereich des Bundesministeriums des Innern ersatzlos gestrichen worden. Der akkreditierte Diensteanbieter hatte der Behörde hierbei unverzüglich eine Versandbestätigung nach § 5 Abs. 7 De-Mail-G und eine Abholbestätigung nach § 5 Abs. 9 De-Mail-G zu übermitteln. Letztere genügte zum Nachweis der elektronischen Zustellung (§ 5a Abs. 3 Satz 1 VwZG a.F.). Wurde das Verfahren auf Verlangen des Empfängers in elektronischer Form abgewickelt, griff bei Ausbleiben der Abholbestätigung eine widerlegliche Zustellungsfiktion, die an die Absendung an das De-Mail-Postfach des Empfängers anknüpfte (§ 5a Abs. 4 VwZG a.F.).

[241] Sander/Smollich, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 5 VwZG, Rn. 6-8.

2.3.4. Folgerungen für die Architektur von ZaPuK

- Die Zustellung an einen Empfängerkreis – für den keine Erleichterungen nach § 5 Abs. 4 VwZG gelten – setzt voraus, dass die zustellende Behörde das zuzustellende elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen kann (§ 5 Abs. 5 Satz 3 VwZG). Soll das zum Nachweis der Zustellung erforderliche Empfangsbekenntnis elektronisch erteilt und an die Behörde zurückübermittelt werden, bedarf auch dieses einer qualifizierten elektronischen Signatur des Ausstellers. Daraus folgt jedoch nicht, dass die Erzeugung qualifizierter elektronischer Signaturen zwingend zum Funktionsumfang von ZaPuK gehören muss. Ausreichend ist vielmehr, dass das System die unveränderte Übermittlung extern und eigenverantwortlich signierter Dokumente ermöglicht (vgl. ADR-0017, Abschnitt 5.4.12 und 5.5.4 des Konzepts).

- Der Befund zum Empfangsbekenntnis stützt die Architekturentscheidung zugunsten verschlüsselter anwendungsspezifischer Events, die neben einer automatischen Bereitstellungs- oder Abrufbestätigung auch eine aktive Lesebestätigung (ANF_FUN_ZUS_048) und deren Erweiterbarkeit zum elektronischen Empfangsbekenntnis unter Wahrung der E2EE-Konformität (SIC_VER_ÜBE_032) umfasst (ADR-1118). Denn über eine automatische Bereitstellungs- oder Abrufbestätigung kann der erforderliche Annahmewille des Empfängers nicht abgebildet werden. Für die aktive Lesebestätigung soll dabei ein eigener Event-Typ definiert werden, der eine aktive Mitwirkungshandlung des Empfängers im Client voraussetzt. Um dem voluntativen Element des Empfangsbekenntnisses ausreichend Rechnung zu tragen, sollte es dem Empfänger hierbei allerdings möglich sein, auch das Zustellungsdatum eigenständig anzugeben, da dieses vom tatsächlichen Abruf- oder Anzeigezeitpunkt abweichen kann (siehe hierzu auch D.VI.4.).

3. Umsetzung des Schriftformerfordernisses bei elektronischer Kommunikation

Kurzzusammenfassung: Die Verwaltungsverfahrensordnungen des Bundes (VwVfG, SGB I, AO) sehen jeweils vor, dass eine durch Rechtsvorschrift angeordnete Schriftform grundsätzlich auch durch die elektronische Form ersetzt werden kann.

Auf Seiten der Bürgerinnen und Bürger bestehen für den Schriftformersatz bislang insbesondere folgende Möglichkeiten: die Anbringung einer qualifizierten elektronischen Signatur, die unmittelbare Abgabe der Erklärung in einem von der Behörde über öffentlich zugängliche Netze zur Verfügung gestellten elektronischen Formular unter Einsatz eines elektronischen Identitätsnachweises sowie – in Verfahren nach dem VwVfG und dem SGB – die Übermittlung einer einfach elektronisch signierten Erklärung aus einem Postfach aus dem EGVP-Verbund. Für Behörden besteht aktuell nur die Möglichkeit, die Schriftform durch Anbringung einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels zu ersetzen. Eine Besonderheit gilt im Bereich der Steuerverwaltung: Gemäß § 87a Abs. 4 Satz 2 AO genügt der elektronischen Form auch ein elektronischer Verwaltungsakt, der in einem sicheren Verfahren nach § 87a Abs. 7 oder 8 AO durch die Finanzbehörden übermittelt oder zum Abruf bereitgestellt wird.

Im VwVfG tritt zum 1. Juli 2027 allerdings eine Änderung in Kraft. § 3a VwVfG erhält eine neue Fassung und wird um einen § 3b und einen § 3c VwVfG n.F. ergänzt. Künftig genügt nach § 3a Abs. 2 VwVfG n.F. zur Wahrung einer gesetzlich angeordneten Schriftform grundsätzlich bereits ein elektronisches Dokument, sofern das Fachrecht keine abweichenden Anforderungen vorsieht. Soweit das Fachrecht die elektronische Form nach § 3b VwVfG n.F. dagegen ausdrücklich vorschreibt, kann diese auf drei Wegen gewahrt werden: durch die unmittelbare Abgabe einer Erklärung in einem von der Behörde bereitgestellten elektronischen Formular nach vorheriger Identitätsfeststellung, durch ein mit qualifizierter elektronischer Signatur der erklärenden Person oder einem qualifizierten elektronischen Siegel der Behörde versehenes elektronisches Dokument oder durch Einreichung auf einem sicheren Übermittlungsweg nach § 3c VwVfG n.F. Sichere Übermittlungswege müssen gewährleisten, dass sie auf einem, dem jeweiligen Stand der Technik entsprechenden, Protokollstandard beruhen, die Identität der erklärenden Person festgestellt worden ist und sich die erklärende Person zur Übermittlung eines elektronischen Dokuments authentisiert. Die Anerkennung von ZaPuK als sicherer Übermittlungsweg setzt nach künftigem Recht die Festlegung durch Rechtsverordnung nach § 3c Abs. 2 VwVfG n.F. voraus.

3.1. Bislang geltende Rechtslage

3.1.1. Bei an die Behörde gerichteten elektronischen Erklärungen

Besteht für eine gegenüber der Behörde abzugebende Erklärung ein gesetzliches Schriftformerfordernis (z.B. für die Einlegung eines Widerspruchs[242]), schließt dies eine elektronische Abgabe nicht aus. Voraussetzung ist jedoch, dass die Erklärung in einer gesetzlich vorgesehenen Form abgegeben wird, die die Schriftform ersetzt.

Nach den Verwaltungsverfahrensordnungen des Bundes kann eine durch Rechtsvorschrift angeordnete Schriftform grundsätzlich durch die elektronische Form ersetzt werden, der nach den Bestimmungen der §§ 3a Abs. 2 VwVfG, 87a Abs. 3 AO und 36a Abs. 2 SGB I ein mit einer qualifizierten elektronischen Signatur versehenes elektronisches Dokument genügt.

Darüber hinaus kann die Schriftform durch die unmittelbare Abgabe der Erklärung in einem elektronischen Formular ersetzt werden, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird (§§ 3a Abs. 3 Nr. 1 VwVfG, 87a Abs. 3 Satz 4 und 5 sowie § 36a Abs. 2a Nr. 1 SGB I). Erfolgt die Eingabe über öffentlich zugängliche Netze, ist ein elektronischer Identitätsnachweis erforderlich. Im Verhältnis zwischen Versicherten und Krankenkassen kann der Nachweis der Identität auch mittels elektronischer Gesundheitskarte (§ 291a SGB V) oder der digitalen Identität (§ 291 Abs. 8 SGB V) geführt werden. Im allgemeinen Verwaltungsverfahrensrecht und im Sozialverwaltungsverfahrensrecht besteht daneben die Möglichkeit, eine elektronisch signierte Erklärung an die Behörde aus einem der in § 3a Abs. 3 Nr. 2 lit. a bis c VwVfG bzw. § 36a Abs. 2a Nr. 2 lit. a bis c SGB I aufgezählten Postfächer zu übermitteln, die auf der für den elektronischen Rechtsverkehr mit den Gerichten etablierten Infrastruktur des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP) beruhen (z.B. das besondere elektronische Anwaltspostfach (beA), das besondere elektronische

[242] Die Einlegung von Widersprüchen im Verwaltungsverfahrensrecht richtet sich nach § 70 Abs. 1 VwGO, der hinsichtlich der elektronischen Form auf § 3a Abs. 2 VwVfG und hinsichtlich des Schriftformersatzes auf § 3a Abs. 3 VwVfG und § 9a Abs. 5 OZG verweist.

Behördenpostfach (beBPo) oder das besondere elektronische Bürger- und Organisationspostfach (eBO)). Ausreichend ist dabei die einfache Namenswiedergabe der erklärenden Person.[243]

Schließlich kann die Schriftform bei Nutzung eines OZG-Nutzerkontos auch dadurch ersetzt werden, dass der Nutzer nach erfolgtem Identitätsnachweis seine Erklärung mittels eines Online-Formulars über ein Verwaltungsportal abgibt (§ 9a Abs. 5 OZG).

3.1.2. Bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde

Das Verwaltungsverfahren kann im Grundsatz behördenseitig formfrei ausgestaltet werden. Gemäß §§ 10 VwVfG und 9 SGB X ist es an bestimmte Formen nicht gebunden, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen.[244]

Ist durch Rechtsvorschrift die Schriftform angeordnet, kann diese im Rahmen der digitalen Kommunikation behördenseitig derzeit grundsätzlich nur durch eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel ersetzt werden (§§ 3a Abs. 2 und 3 Nr. 3 VwVfG, 87a Abs. 4 AO, 36a Abs. 2 und 2a Nr. 3 SGB I sowie 9a Abs. 6 OZG). Allerdings genügt im Bereich der Steuerverwaltung auch die Übermittlung oder Bereitstellung des Verwaltungsakts zum Abruf in einem sicheren Verfahren nach § 87a Abs. 7 oder 8 AO (§ 87a Abs. 4 Satz 2 AO). Die bislang vorgesehene Möglichkeit, die Schriftform durch Versendung einer De-Mail-Nachricht zu ersetzen, ist mit dem Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern entfallen.

[243] Schulz, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 3. Auflage 2025, § 3a, Rn. 137 bis 143.

[244] Tiedemann, in: BeckOK VwVfG, Bader/Ronellenfitsch, 69. Edition, Stand: 01.10.2025, § 37, Rn. 25; besondere Regelungen trifft das VwVfG in den §§ 63 ff. für das förmliche Verwaltungsverfahren, dort unter anderem in § 69 Abs. 2 VwVfG zur Form von Verwaltungsakten. Gemäß § 69 Abs. 2 Satz 2 VwVfG ist ein elektronischer Verwaltungsakt, der das förmliche Verfahren abschließt, mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur zu versehen.

3.2. Neuordnung durch das Gesetz für den Bürokratierückbau zum 1. Juli 2027

Mit dem Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern wird der aktuelle § 3a VwVfG mit Wirkung zum 1. Juli 2027 neu gefasst und um die neuen §§ 3b und 3c VwVfG n.F. ergänzt.

Nach dem neuen § 3a Abs. 2 VwVfG n.F. wird eine durch Rechtsvorschrift angeordnete Schriftform bereits durch ein elektronisches Dokument gewahrt, soweit durch Rechtsvorschrift nichts anderes – insbesondere nicht die elektronische Form nach dem neu eingefügten § 3b VwVfG n.F. – bestimmt ist. Bestehen Zweifel an der Authentizität oder der Integrität eines elektronischen Dokuments, so kann die Behörde einen geeigneten Identitätsnachweis oder dessen Vorlage in anderer Form verlangen (§ 3a Abs. 3 Satz 1 VwVfG n.F.). Der Zeitraum vom Zugang der Nachforderung bis zum Eingang der Antwort hierauf wird nicht auf den Lauf einer Frist gegenüber der Behörde eingerechnet (§ 3a Abs. 3 Satz 2 VwVfG n.F.). Ausweislich der Gesetzesbegründung orientiert sich der in § 3a Abs. 2 VwVfG n.F. verwendete Begriff des „elektronischen Dokuments" an dem zivilrechtlichen Begriff der Textform (§ 126b BGB). Die vergleichsweise hohen Hürden für den Schriftformersatz sollen damit im Grundsatz entfallen. Abweichende Anforderungen bleiben einer ausdrücklichen fachrechtlichen Regelung vorbehalten. Stellt das Fachrecht solche abweichenden Anforderungen auf, kann die Schriftform durch die elektronische Form nach Maßgabe des neuen § 3b VwVfG n.F. ersetzt werden.[245]

Die elektronische Form nach § 3b Satz 1 VwVfG n.F. wird durch ein elektronisches Dokument gewahrt, das

- nach Feststellung der Identität der erklärenden Person als Erklärung in einem elektronischen Formular unmittelbar abgegeben wird, das von der Behörde in einem Eingabegerät oder über öffentliche zugängliche Netze zur Verfügung gestellt wird (Nr. 1),

[245] Begründung zu § 3a VwVfG n.F., Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksache 21/3620 – vom 20.05.2026, Drucksache 21/6049, S. 22.

- unabhängig vom Übermittlungsweg mit einer qualifizierten elektronischen Signatur der erklärenden Person oder einem qualifizierten elektronischen Siegel der Behörde versehen ist; die Signierung mit einem Pseudonym ist nicht zulässig (Nr. 2), oder
- auf einem sicheren Übermittlungsweg nach § 3c VwVfG n.F. eingereicht wird (Nr. 3).

Sichere Übermittlungswege müssen nach § 3c Abs. 1 VwVfG n.F. gewährleisten, dass

- sie auf einem, dem jeweiligen Stand der Technik entsprechenden, Protokollstandard beruhen (Nr. 1),
- die Identität der erklärenden Person festgestellt worden ist (Nr. 2) und
- sich die erklärende Person zur Übermittlung eines elektronischen Dokuments authentisiert (Nr. 3).

§ 3c Abs. 2 VwVfG n.F. enthält eine Verordnungsermächtigung zur Festlegung der sicheren Übermittlungswege. Danach werden die sicheren Übermittlungswege einschließlich der zum Nachweis zugelassenen Identifizierungsmittel nach § 3c Abs. 1 Nr. 2 und § 3b Satz 1 Nr. 1 VwVfG n.F. durch Rechtsverordnung des Bundesministeriums des Innern im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung ohne Zustimmung des Bundesrates festgelegt.

Ausgehend vom Wortlaut der neuen §§ 3b Satz 1 Nr. 3 und 3c Abs. 1 VwVfG n.F. dürfte die Nutzung eines sicheren Übermittlungswegs allerdings nur für den „Hinkanal" – also für gegenüber der Behörde abgegebene Erklärungen – schriftformersetzend wirken. Denn § 3b Satz 1 Nr. 3 VwVfG n.F. stellt auf elektronische Dokumente ab, die auf einem sicheren Übermittlungsweg nach § 3c VwVfG n.F. „eingereicht" werden. Die Regelung erfasst ihrem Wortlaut nach damit nur die Übermittlung eines elektronischen Dokuments an die Behörde. Die umgekehrte Übermittlungsrichtung – der „Rückkanal" – wird demgegenüber nicht erfasst. Weshalb die Neuregelung insoweit zwischen Hin- und Rückkanal differenziert, bleibt offen.

Vor diesem Hintergrund wäre zu erwägen, den Anwendungsbereich der §§ 3b Satz 1 Nr. 3 und 3c Abs. 1 VwVfG n.F. noch vor deren Inkrafttreten auf die behördenseitige Übermittlung

elektronischer Dokumente zu erstrecken. Darüber hinaus erscheint es sinnvoll, entsprechende Regelungen über sichere Übermittlungswege auch in § 87a AO und § 36a SGB I vorzusehen.

3.3. Folgerungen für die Architektur von ZaPuK

- Soweit die geltende Rechtslage eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel für den Ersatz der Schriftform erfordert, ermöglicht die ZaPuK-Architektur die unveränderte Übermittlung der vom jeweiligen Absender eigenverantwortlich signierten bzw. gesiegelten Dokumente als Dateianhänge (vgl. ADR-0017, Abschnitt 5.4.12 und 5.5.4 des Konzepts).

- Die Anerkennung von ZaPuK als sicherer Übermittlungsweg im Sinne von §§ 3b Satz 1 Nr. 3 und 3c Abs. 1 VwVfG n.F setzt danach die Festlegung durch Rechtsverordnung des BMI im Einvernehmen mit dem BMDS nach § 3c Abs. 2 VwVfG n.F. voraus.

III. Datenschutzrechtliche Rahmenbedingungen für die Umsetzbarkeit von ZaPuK

Das Datenschutzrecht dient dazu, die Grundrechte der Personen, die von einer Datenverarbeitung betroffen sind, zu schützen – insbesondere das Grundrecht auf Datenschutz bzw. „informationelle Selbstbestimmung".[246] Hierzu erlegt das Datenschutzrecht den Akteuren, die an einer Verarbeitung personenbezogener Daten beteiligt sind, Pflichten auf. Da die Nutzungsszenarien von ZaPuK mit einer Verarbeitung personenbezogener Daten verbunden sind, ergeben sich aus dem Datenschutzrecht Anforderungen für die Beteiligten – also insbesondere für die Einzelpersonen und Organisationen, welche Postfächer zum Empfang und Versand von Nachrichten nutzen, sowie für die Betreiber der Infrastruktur. Diese Anforderungen sind bei der Konzeption von ZaPuK zu beachten. ZaPuK muss die Erfüllung dieser Anforderungen ermöglichen und sollte sie darüber hinaus weitestgehend erleichtern und unterstützen.

[246] Vgl. Art. 1 DSGVO und Art. 8 EU-Grundrechteharta. Das Grundrecht auf „informationelle Selbstbestimmung" wird in Deutschland aus Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG hergeleitet (maßgeblich ist das Volkszählungsurteil des BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83).

1. Anwendbares Datenschutzrecht

1.1. Unionsrecht

Kurzzusammenfassung. Das für ZaPuK maßgebliche Datenschutzrecht ist unionsrechtlich geprägt und in seinem Kern durch die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO") weitgehend vereinheitlicht. Die DSGVO gilt als Verordnung unmittelbar und erfasst die Datenverarbeitung in Wirtschaft und Verwaltung sowie grundsätzlich auch in der Justiz. Sie bildet damit den vorrangigen Rechtsrahmen für das Gros der ZaPuK-Nutzungsszenarien und gibt die Grundsätze vor, an denen die Architektur auszurichten ist.

Vom sachlichen Anwendungsbereich der DSGVO ausgenommen ist die Datenverarbeitung der zuständigen Behörden zu Zwecken der Strafverfolgung und Gefahrenabwehr; dieser Bereich wird durch die JI-Richtlinie harmonisiert, die im Bundesdatenschutzgesetz (BDSG) und den Landesdatenschutzgesetzen umgesetzt ist und im Wesentlichen denselben Grundsätzen folgt.

Ergänzend ist für die Kommunikationsfunktion von ZaPuK das unionsrechtliche Regime zum Schutz der elektronischen Kommunikation (ePrivacy-Richtlinie) zu beachten, das der DSGVO nach deren Art. 95 vorgeht, soweit dieselben Pflichten betroffen sind.

Die DSGVO regelt den Datenschutz nicht abschließend, sondern lässt dem nationalen Gesetzgeber über Öffnungsklauseln – insbesondere für Verarbeitungen öffentlicher Stellen – Gestaltungsspielräume; das hierauf beruhende nationale Recht wird im nachfolgenden Abschnitt behandelt (siehe 1.2).

1.1.1. Die DSGVO als vorrangiger und weitgehend vereinheitlichter Rahmen

Durch die DSGVO wurde das Datenschutzrecht in der Union weitgehend vereinheitlicht. Als Verordnung gilt sie unmittelbar in allen Mitgliedstaaten und bedarf keiner Umsetzung. Sie schützt gemäß Art. 1 die Grundrechte natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten, welches in der EU-Grundrechtcharta verankert ist. Für ZaPuK folgt daraus, dass die DSGVO den vorrangigen Maßstab bildet und die zentralen Datenschutzprinzipien vorgibt, an denen die Architektur zu messen ist.

Der räumliche Anwendungsbereich (Art. 3 DSGVO) ist für die in Deutschland betriebene, auf inländische Verantwortliche und betroffene Personen ausgerichtete Infrastruktur ohne Weiteres erfüllt. Der sachliche Anwendungsbereich ist weit: Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für deren nichtautomatisierte Verarbeitung in Dateisystemen (Art. 2 Abs. 1 DSGVO). Da über ZaPuK weitgehend personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO – Nachrichteninhalte, Adress- und Kommunikationsmetadaten – verarbeitet werden und der weite Verarbeitungsbegriff des Art. 4 Nr. 2 DSGVO auch die bloße Speicherung, Offenlegung durch Übermittlung und Bereitstellung erfasst, ist der Anwendungsbereich für die ganz überwiegende Zahl der Kommunikationsvorgänge eröffnet. Dass Inhalte Ende-zu-Ende-verschlüsselt transportiert werden, hebt den Anwendungsbereich nicht generell auf – ob verschlüsselte Daten für einen bestimmten Beteiligten personenbezogen sind, beurteilt sich nach dem relativen Maßstab des EuGH danach, ob dieser nach allgemeinem Ermessen wahrscheinlich über Mittel zur Reidentifizierung verfügt, sodass verschlüsselte Daten nicht ausnahmslos für jeden Akteur personenbezogen sind.[247] Zu den Folgen dieses „relativen Personenbezugs" für die einzelnen ZaPuK-Rollen (insbesondere die Backend-Betreiber) siehe 1.3.

Die für die Architektur zentralen materiellen Vorgaben sind bereits in der DSGVO angelegt. Die Verarbeitungsgrundsätze des Art. 5 DSGVO – insbesondere Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit, flankiert durch die Rechenschaftspflicht – bilden den Bewertungsmaßstab für konkrete Fragestellungen zum Datenumgang wie Speicherbegrenzung, Logdaten und Metadaten (siehe 3). Für die technische Ausgestaltung besonders bedeutsam sind Art. 32 DSGVO (Sicherheit der Verarbeitung, siehe 3.6) sowie Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, siehe 5). Beide nennen ausdrücklich Pseudonymisierung und Verschlüsselung als geeignete Maßnahmen und verlangen ein am Stand der Technik und am Risiko orientiertes Schutzniveau. Auf diese Vorschriften stützen sich die architekturprägenden

[247] Vgl. EuGH, C-413/23 P – EDSB/SRB, Rn. 85 f.; grundlegend C-582/14 – Breyer.

Grundentscheidungen von ZaPuK – durchgängige Ende-zu-Ende-Verschlüsselung, Metadatenminimierung und pseudonyme Adressierung – unmittelbar.

1.1.2. Bereichsausnahme und JI-Richtlinie

Vom Anwendungsbereich der DSGVO ausgenommen ist nach Art. 2 Abs. 2 Buchst. d DSGVO die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Dieser Bereich ist nicht ungeregelt, sondern durch die JI-Richtlinie (Richtlinie (EU) 2016/680) harmonisiert. Anders als die DSGVO ist die Richtlinie nicht unmittelbar anwendbar, sondern bedarf der Umsetzung in nationales Recht; diese ist im Bund in Teil 3 des BDSG und in den Ländern in den jeweiligen Landesdatenschutzgesetzen erfolgt. Die JI-Richtlinie verfolgt dieselben Schutzziele – Schutz der Grundrechte und freier Datenaustausch der zuständigen Behörden (Art. 1) – und folgt im Wesentlichen denselben Datenschutzgrundsätzen wie die DSGVO. Sie erlaubt den Mitgliedstaaten ausdrücklich, strengere Garantien vorzusehen (Art. 1 Abs. 3).

Für ZaPuK ist diese Zweiteilung insofern relevant, als die Zielarchitektur eine eigene Teilnehmergruppe und ein eigenes Backend für die Organisationen der Justiz vorsieht. Maßgeblich für die Abgrenzung ist jedoch nicht die Organisation, sondern der Verarbeitungszweck. Nur soweit eine zuständige Behörde zu den in Art. 1 Abs. 1 der JI-Richtlinie genannten Zwecken verarbeitet, gilt das JI-Regime; justizielle Verwaltungstätigkeit und die übrige behördliche Kommunikation unterfallen weiterhin der DSGVO. Da beide Regime auf einem gemeinsamen Grundgerüst beruhen, lässt sich die Architektur an einheitlichen, unionsrechtlich getragenen Anforderungen ausrichten. Zu Besonderheiten des nationalen Rechts siehe 1.2.

1.1.3. Schutz elektronischer Kommunikation (ePrivacy) und Verhältnis zur DSGVO

Neben dem allgemeinen Datenschutzrecht ist für die Kommunikationsfunktion von ZaPuK das unionsrechtliche Sonderregime zum Schutz der Privatsphäre in der elektronischen Kommunikation zu beachten. Die sog. ePrivacy-Richtlinie (Richtlinie 2002/58/EG) verpflichtet die Mitgliedstaaten, die Vertraulichkeit der über öffentlich zugängliche Kommunikationsdienste

übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicherzustellen und insbesondere das Abfangen und Überwachen von Nachrichten ohne Einwilligung zu untersagen (Art. 5 der Richtlinie 2002/58/EG). Diese Vorgaben sind, soweit sie das Fernmeldegeheimnis und den Umgang mit Verkehrs- und Nutzungsdaten betreffen, in Deutschland im Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG) umgesetzt und werden im telekommunikationsrechtlichen Teil vertieft (siehe V).

Das Verhältnis zur DSGVO regelt deren Art. 95: Die DSGVO erlegt in Bezug auf die Verarbeitung im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste keine zusätzlichen Pflichten auf, soweit besondere, dasselbe Ziel verfolgende Pflichten der ePrivacy-Richtlinie bestehen. Für ZaPuK bedeutet dies, dass – soweit ein Postfach als interpersoneller Kommunikationsdienst einzuordnen ist (siehe V) – die spezielleren Vertraulichkeits- und Metadatenregeln vorrangig sind und die DSGVO ergänzend zur Anwendung kommt. Hinzuweisen ist darauf, dass die geplante ePrivacy-Verordnung, die die Richtlinie ablösen und an die DSGVO angleichen soll, bislang nicht in Kraft getreten ist; maßgeblich bleibt daher die Richtlinie in ihrer nationalen Umsetzung (also das TDDDG).

1.1.4. Öffnungsklauseln: kein abschließender Charakter der DSGVO

Die DSGVO regelt den Datenschutz nicht abschließend. Sie enthält zahlreiche Öffnungsklauseln, die den Mitgliedstaaten Gestaltungsspielräume belassen oder eröffnen – für Verarbeitungen öffentlicher Stellen vor allem für die Bereitstellung von Rechtsgrundlagen für Verarbeitungen zur Erfüllung rechtlicher Verpflichtungen und in Ausübung öffentlicher Gewalt. Von diesen Spielräumen hat der deutsche Gesetzgeber im allgemeinen wie im bereichsspezifischen Datenschutzrecht Gebrauch gemacht. Für ZaPuK folgt daraus, dass die unionsrechtlichen Vorgaben zwar den vorrangigen und den Kern bestimmenden Rahmen setzen, die konkrete Zulässigkeit einzelner Verarbeitungen – insbesondere die Rechtsgrundlagen für die Datenverarbeitung öffentlicher Stellen – aber erst im Zusammenspiel mit dem nationalen Recht zu beurteilen ist (dazu 1.2.).

1.1.5. Folgerungen für die Architektur von ZaPuK

Für die ZaPuK-Architektur ergibt sich aus dem Vorstehenden:

- Die DSGVO ist für die meisten ZaPuK-Verarbeitungen der vorrangige und unmittelbar geltende Maßstab. Die Architektur ist konsequent an den Grundsätzen des Art. 5 DSGVO auszurichten. Die bereits getroffenen Grundentscheidungen zu Zweckbindung, Datensparsamkeit und Speicherbegrenzung werden dadurch gestützt.

- Die Grundentscheidungen für durchgängige Ende-zu-Ende-Verschlüsselung, Metadatenminimierung und pseudonyme Adressierung finden in Art. 25 und Art. 32 DSGVO eine unmittelbare unionsrechtliche Grundlage. Sie bilden zudem ein wesentliches Element der Umsetzung von Datenschutz durch Technikgestaltung.

- Die verschlüsselte Übertragung nimmt die Verarbeitung nicht aus dem Anwendungsbereich der DSGVO heraus. Allerdings gilt der relative Begriff des Personenbezugs, sodass verschlüsselte Daten für Akteure, die nicht über die Schlüssel verfügen und diese auch nicht erlangen können, nicht als personenbezogene Daten im Sinne der DSGVO gelten. Für Akteure mit (potentiellem) Zugriff auf die Schlüssel bleibt es insoweit bei den datenschutzrechtlichen Pflichten (u.a. Rechtsgrundlage, technischer Datenschutz, Betroffenenrechte, Rechenschaft).

- Die architektonische Trennung des Justiz-Backends bildet die unionsrechtliche Zweiteilung zwischen DSGVO und JI-Richtlinie sinnvoll ab, determiniert das anwendbare Regime aber nicht abschließend. Maßgeblich bleibt der jeweilige Verarbeitungszweck. Da beide Regime auf gemeinsamen Grundsätzen beruhen, sollte die Konformität gegen diesen gemeinsamen Kern nachgewiesen werden.

- Für die Postfach-/Kommunikationsfunktion ist wegen Art. 95 DSGVO das ePrivacy-Regime (Vertraulichkeit, Verkehrs-/Metadaten) vorrangig mitzudenken. Dies stützt die metadatensparsame Ausgestaltung und wird im TK-rechtlichen Teil vertieft (siehe V).

- Weil die DSGVO über Öffnungsklauseln auf mitgliedstaatliches Recht verweist, ist die abschließende Beurteilung der Rechtsgrundlagen und bereichsspezifischen Anforderungen erst unter Berücksichtigung des nationalen Rechts möglich. Zu einzelnen Fragen wäre eine spezialgesetzliche Absicherung unter dem Gesichtspunkt der Rechtssicherheit wünschenswert (siehe 3.6.3 und 2.2).

1.2. Nationales Recht

Kurzzusammenfassung. Die DSGVO gilt für ZaPuK unmittelbar, lässt dem nationalen Gesetzgeber über die Öffnungsklauseln der Art. 6 Abs. 2 und Abs. 3 DSGVO aber Raum für „spezifischere Bestimmungen", insbesondere für Verarbeitungen im öffentlichen Interesse und in Ausübung öffentlicher Gewalt. Welches nationale Datenschutzrecht auf eine konkrete Verarbeitung innerhalb der ZaPuK-Infrastruktur anwendbar ist, lässt sich nicht einheitlich beantworten. Es richtet sich nach der jeweils verantwortlichen Stelle und dem betroffenen Verarbeitungskontext. Für Bundesstellen gilt das BDSG, für Landes- und Kommunalstellen grundsätzlich das jeweilige Landesdatenschutzgesetz, und bereichsspezifische Geheimnis- und Datenschutzregime (Sozialdatenschutz, Steuergeheimnis, Fernmeldegeheimnis, Justiz/JI-Recht) gehen dem allgemeinen Datenschutzrecht jeweils vor. ZaPuK trifft als domänenagnostische Kommunikationsinfrastruktur (ADR-0001) selbst keine Aussage darüber, welches dieser Regime greift. Die Architektur muss vielmehr so ausgelegt sein, dass sie den Anforderungen aller in Betracht kommenden Regime – einschließlich der strengsten – gerecht wird.

1.2.1. Nationales Recht im Gefüge der DSGVO

Die DSGVO ist als Verordnung unmittelbar anwendbar und bildet den vorrangigen Rechtsrahmen (Art. 288 Abs. 2 AEUV; § 1 Abs. 5 BDSG). Nationales Datenschutzrecht kommt nur insoweit zur Anwendung, als die DSGVO es ausdrücklich zulässt oder gebietet. Für die hier maßgeblichen Verarbeitungen öffentlicher Stellen eröffnen vor allem Art. 6 Abs. 2 und Abs. 3 DSGVO einen mitgliedstaatlichen Gestaltungsspielraum: Die Mitgliedstaaten dürfen für Verarbeitungen zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) und für Verarbeitungen in Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e DSGVO) „spezifischere Bestimmungen" beibehalten oder

einführen. Dabei ist anerkannt, dass diese Öffnungsklauseln erheblichen Spielraum eröffnen, nationale Regelungen das Schutzniveau der DSGVO aber weder unterschreiten noch deren Wortlaut lediglich wiederholen dürfen.[248]

Für ZaPuK folgt daraus, dass das nationale Recht die datenschutzrechtlichen Vorgaben der DSGVO nicht ersetzt, sondern konkretisiert und ergänzt – insbesondere durch bereichsspezifische Rechtsgrundlagen, Zweckbindungen und Geheimhaltungspflichten. Neben der DSGVO ist die auf den Bereich der Strafverfolgung und Gefahrenabwehr bezogene JI-Richtlinie (RL (EU) 2016/680) zu beachten, die nicht unmittelbar gilt, sondern nationaler Umsetzung bedarf (dazu unten 1.2.4).

1.2.2. Allgemeines Datenschutzrecht: BDSG und Landesdatenschutzgesetze

Das allgemeine, „vor die Klammer gezogene" nationale Datenschutzrecht ist zweigeteilt. Nach § 1 Abs. 1 BDSG gilt das Bundesdatenschutzgesetz für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes sowie – nur subsidiär – durch öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege in Nicht-Verwaltungsangelegenheiten tätig werden. Wer öffentliche Stelle des Bundes bzw. des Landes ist, bestimmt § 2 BDSG. Erfasst sind auch Gemeinden und Gemeindeverbände als öffentliche Stellen der Länder (§ 2 Abs. 2 BDSG).

In der Praxis bedeutet dies, dass für die ganz überwiegende Zahl der an ZaPuK teilnehmenden Verwaltungsträger – Landes- und Kommunalbehörden – nicht das BDSG, sondern das jeweilige Landesdatenschutzgesetz maßgeblich ist, da die Länder im Rahmen des vom DSGVO eröffneten Gestaltungsspielraums ihren Datenschutz eigenständig geregelt haben. Die Landesgesetze orientieren sich zwar weitgehend am BDSG, weichen aber im Detail voneinander ab.

[248] Kramer, in: Auernhammer, DSGVO/BDSG, 8. Aufl. 2024, Art. 6 DSGVO, Rn. 10, 123.

Für nichtöffentliche Stellen – also private Organisationen und Privatpersonen als Teilnehmer – gilt unmittelbar die DSGVO, ergänzt um die für nichtöffentliche Stellen einschlägigen Vorschriften des BDSG (§ 1 Abs. 4 BDSG).

Für das allgemeine Datenschutzrecht gilt zudem der Subsidiaritätsgrundsatz: Nach § 1 Abs. 2 BDSG gehen andere – insbesondere bereichsspezifische – Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor. Nur soweit sie einen Sachverhalt nicht oder nicht abschließend regeln, greift das BDSG ergänzend.

1.2.3. Bereichsspezifisches Datenschutz- und Geheimnisrecht

Da ZaPuK bereichsübergreifend eingesetzt werden soll, ist das bereichsspezifische Datenschutzrecht von besonderer Bedeutung. Es verdrängt in seinem Anwendungsbereich das allgemeine Datenschutzrecht und stellt teils erheblich strengere Anforderungen an Vertraulichkeit, Zweckbindung und Übermittlung. Für die im Architekturkonzept ausdrücklich adressierten Fachlichkeiten sind hervorzuheben der Sozialdatenschutz, das Steuergeheimnis und ggf. weitere Geheimnisschutztatbestände.

a) Sozialdatenschutz

Für Sozialdaten – d.h. für personenbezogene Daten, die von einem Leistungsträger im Hinblick auf seine Aufgaben nach dem SGB verarbeitet werden (§ 67 Abs. 2 SGB X) – regeln das Zweite Kapitel des SGB X und die übrigen Bücher des Sozialgesetzbuchs die Verarbeitung abschließend, soweit nicht die DSGVO unmittelbar gilt (§ 35 Abs. 2 SGB I). Es besteht ein besonderes Sozialgeheimnis (§ 35 Abs. 1 SGB I), das auch innerorganisatorisch die Beschränkung des Zugriffs auf Befugte verlangt. Für die Ausgestaltung der Kommunikation über ZaPuK ist dies insbesondere im Hinblick auf Vertretungs- und Archivierungslösungen sowie den serverseitigen Zugriff technischer Nutzer relevant.

b) Steuergeheimnis

Für die Steuerverwaltung tritt das Steuergeheimnis nach § 30 AO hinzu, das Amtsträgern die unbefugte Offenbarung, Verwertung oder den unbefugten Abruf geschützter Daten untersagt.

§ 30 AO enthielt überdies bis Juli 2026 eine ausdrückliche Wertung zur Verschlüsselung: Eine kurzzeitige automatisierte Entschlüsselung durch einen akkreditierten De-Mail-Diensteanbieter zur Schadsoftwareprüfung und Weiterleitung galt danach nicht als unbefugte Offenbarung (§ 30 Abs. 7 AO a.F.). Diese Wertung ist für die Frage bedeutsam, ob und wie eine serverseitige Verarbeitung verschlüsselter Inhalte im ZaPuK-Kontext zulässig wäre (dazu 3.6.2).

c) Weitere Geheimnisschutztatbestände

§ 1 Abs. 2 Satz 3 BDSG und die Parallelvorschriften stellen klar, dass gesetzliche Geheimhaltungspflichten sowie Berufs- und besondere Amtsgeheimnisse unberührt bleiben. Für die von ZaPuK adressierten Nutzergruppen kommen daher – je nach Kommunikationsbeziehung – auch berufsrechtliche Verschwiegenheitspflichten (etwa der steuerberatenden und rechtsberatenden Berufe) in Betracht.

1.2.4. Datenschutz im Bereich der Justiz und der Strafverfolgung (JI-Recht)

Soweit zuständige öffentliche Stellen personenbezogene Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten verarbeiten, gilt nicht die DSGVO, sondern das zur Umsetzung der JI-Richtlinie geschaffene besondere Datenschutzregime – auf Bundesebene Teil 3 des BDSG (§§ 45 ff. BDSG), auf Landesebene die entsprechenden Landesumsetzungen. Diese Abgrenzung ist für ZaPuK insofern relevant, als eine eigene Teilnehmergruppe und ein eigenes Backend – bzw. ein eigener Homeserver – für die Organisationen der Justiz vorgesehen sind (vgl. Architekturkonzept, Abschnitt 4.2.3.2). Zu beachten ist dabei, dass sich der Anwendungsbereich des JI-Rechts nicht nach der Organisation, sondern nach dem Verarbeitungszweck bestimmt; justizielle Verwaltungsangelegenheiten unterfallen weiterhin dem allgemeinen Datenschutzrecht. Für die Architektur bedeutet dies, dass die Zuordnung einer Kommunikation zum Justiz-Backend das anwendbare Datenschutzregime nicht abschließend determiniert.

1.2.5. Telekommunikations- und telemedienbezogenes Datenschutzrecht

Soweit ein ZaPuK-Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu ausführlich V), treten die spezialgesetzlichen Vorgaben des TDDDG hinzu, insbesondere

das Fernmeldegeheimnis nach § 3 TDDDG. Dieses schützt den Inhalt der Telekommunikation und ihre näheren Umstände, ausdrücklich auch die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist (§ 3 Abs. 1 TDDDG), und beschränkt die Kenntnisnahme und Verwendung durch die Verpflichteten auf das für die Diensterbringung erforderliche Maß (§ 3 Abs. 3 TDDDG). Für das Verhältnis zur DSGVO ist Art. 95 DSGVO maßgeblich: Die DSGVO erlegt keine zusätzlichen Pflichten auf, soweit besondere, dasselbe Ziel verfolgende Pflichten der e-Privacy-Richtlinie (und ihrer nationalen Umsetzung) bestehen. Das telekommunikationsbezogene Datenschutzrecht ist damit für die metadatensparsame Ausgestaltung der Infrastruktur von hoher Bedeutung und wird im TK-rechtlichen Teil vertieft.

1.2.6. Bereichsspezifische Rechtsgrundlagen mit Bezug zur Postfachinfrastruktur

Der nationale Gesetzgeber hat für die Verwaltungsdigitalisierung bereits spezifische datenschutzrechtliche Rechtsgrundlagen und Verantwortlichkeitszuweisungen geschaffen, die als Referenz für ZaPuK dienen können. So regelt § 8 OZG die Rechtsgrundlagen der Datenverarbeitung in Nutzerkonten und zu Identifizierungszwecken, und § 8a OZG weist die datenschutzrechtliche Verantwortlichkeit für den länderübergreifenden Onlinedienst ausdrücklich zu (§ 8a Abs. 4 OZG). Diese Regelungstechnik – die spezialgesetzliche Klarstellung der Verantwortlichkeit in einer verteilten Infrastruktur – ist für die im Rahmen von ZaPuK zu klärende Verantwortlichkeit in einem verteilten Mehr-Betreiber-System von unmittelbarer Bedeutung (dazu näher 2.2).

1.2.7. Folgerungen für die Architektur von ZaPuK

Für die ZaPuK-Architektur ergibt sich aus dem Vorstehenden:

- Die Entscheidung, ZaPuK als domänenagnostische Kommunikationsinfrastruktur ohne fachspezifische Logik auszugestalten (ADR-0001), ist aus datenschutzrechtlicher Sicht folgerichtig und wird bestätigt: Das innerhalb des nationalen Rechts anwendbare Datenschutzregime bestimmt sich nach der verantwortlichen Stelle und dem Verarbeitungskontext. Dem wird eine domänenagnostische und insoweit offene/flexible Infrastruktur gerecht.

- Die Aufteilung in getrennte Backends je Teilnehmergruppe (Privatpersonen, private Organisationen, öffentliche Stellen, Justiz) bildet die unterschiedlichen Verantwortlichkeits- und Regimezuordnungen sinnvoll ab und unterstützt die Metadatentrennung. Sie determiniert das anwendbare Datenschutzrecht jedoch nicht abschließend – in Bezug auf die öffentlichen Stellen bleibt die Unterscheidung zwischen BDSG, Landesrecht und bereichsspezifischem Recht (Sozial, Steuer, Justiz/JI) bestehen.

- Weil ZaPuK zugleich Verarbeitungen unter besonders strengen Geheimnisregimen (§ 30 AO, § 35 SGB I, § 3 TDDDG) ermöglichen muss, ist die Architektur am jeweils höchsten Schutzniveau auszurichten. Die vorgesehene durchgängige Ende-zu-Ende-Verschlüsselung und die Metadatenminimierung sind hierfür geeignete und angemessene Maßnahmen.

- Angesichts der Geltung von bis zu sechzehn Landesdatenschutzgesetzen neben dem BDSG sollte die Konformität nicht gegen ein einzelnes Regime, sondern abstrahiert gegen die gemeinsamen, DSGVO-getragenen Anforderungen nachgewiesen werden. Verbindliche Vorgaben gegenüber den teilnehmenden Stellen sind über die Anschlussbedingungen (ADR-1145) zu transportieren, ohne die eigenständige datenschutzrechtliche Verantwortung der jeweiligen Stelle zu verlagern.

- Für bereichsübergreifende Verarbeitungen (insbesondere die Zuweisung der datenschutzrechtlichen Verantwortlichkeit im verteilten Betrieb sowie der Schutz von Kommunikationsmetadaten) empfiehlt sich – dem Vorbild des § 8a OZG folgend – die Prüfung einer spezialgesetzlichen Verankerung. Dies schafft Rechtssicherheit gegenüber der kasuistischen Beurteilung nach den Öffnungsklauseln (siehe 3.6.3 und 2.2).

1.3. Anwendbarkeit

Kurzzusammenfassung. Der sachliche Anwendungsbereich der DSGVO ist für ZaPuK dem Grunde nach eröffnet, weil nahezu jeder Vorgang in der Infrastruktur – Erheben, Speichern, Offenlegen durch Übermittlung und Bereitstellen – eine Verarbeitung im Sinne des weiten Verarbeitungsbegriffs des Art. 4 Nr. 2 DSGVO darstellt. Ob eine konkrete Verarbeitung dem

Datenschutzrecht unterliegt, hängt aber davon ab, ob die verarbeiteten Daten *für den jeweiligen Akteur* personenbezogen sind. Maßgeblich ist insoweit der relative Begriff des Personenbezugs, der durch die Rechtsprechung des EuGH – zuletzt in der Sache EDSB/SRB – mittlerweile bestätigt ist: Dieselbe Information kann für den einen Beteiligten personenbezogen und für den anderen anonym sein. Für ZaPuK bedeutet dies eine nach Rolle und Datenart differenzierte Betrachtung. Die durchgängige Ende-zu-Ende-Verschlüsselung führt dazu, dass die *Inhaltsdaten* für die reinen Transport- und Speicherakteure (insbesondere die Backend-Betreiber ohne Schlüsselzugriff) nicht als personenbezogene Daten gelten und die Verarbeitung insoweit nicht der DSGVO unterfällt. Die *Kommunikationsmetadaten* bleiben dagegen auch bei pseudonymer Adressierung für diese Betreiber personenbezogen. Uneingeschränkt anwendbar bleibt das Datenschutzrecht überall dort, wo Klartext anfällt – an den Endgeräten, bei serverseitigen Entschlüsselungsendpunkten (technische Nutzer, Organisationsgrenze) und bei den versendenden Stellen.

1.3.1. Ausgangspunkt: weiter Verarbeitungsbegriff, aber relativer Personenbezug

Die DSGVO gilt nach Art. 2 Abs. 1 DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Beide Tatbestandsmerkmale sind für ZaPuK gesondert zu prüfen.

a) Verarbeitungsbegriff (Art. 4 Nr. 2 DSGVO)

Der Verarbeitungsbegriff des Art. 4 Nr. 2 DSGVO ist bewusst weit gefasst und erfasst ausdrücklich auch die bloße Speicherung, das Auslesen, die Offenlegung durch Übermittlung und jede sonstige Form der Bereitstellung. Schon deshalb bildet nahezu jeder technische Vorgang innerhalb der Infrastruktur – das Annehmen einer Nachricht durch ein Postfach-Backend, ihr Vorhalten in verschlüsselter Form, ihre Weiterleitung im Verbund, die Erzeugung von Quittungen – tatbestandlich eine Verarbeitung. Der Anwendungsbereich lässt sich daher nicht über den Verarbeitungsbegriff, sondern allein über das Merkmal des Personenbezugs der jeweils verarbeiteten Daten eingrenzen.

b) Personenbezogene Daten (Art. 4 Nr. 1 DSGVO) – Betrachtung aus der Sicht der verarbeitenden Stelle ("relativer Personenbezug")

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist, wer direkt oder indirekt bestimmt werden kann. Für die Frage, wann eine Person „identifizierbar" ist, verweist ErwGr. 26 DSGVO auf „alle Mittel …, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden", wobei objektive Faktoren wie Kosten und Zeitaufwand sowie der Stand der Technik heranzuziehen sind. Zugleich stellt ErwGr. 26 Satz 5 klar, dass die Grundsätze des Datenschutzes für anonyme Informationen nicht gelten.

Aus diesem Maßstab folgt der *relative* Charakter des Personenbezugs. Nach der in Rechtsprechung und Literatur inzwischen ganz überwiegend vertretenen Auffassung kommt es nicht darauf an, ob *irgendjemand* die Person bestimmen könnte, sondern darauf, ob die konkret handelnde Stelle über Mittel verfügt, die sie nach allgemeinem Ermessen wahrscheinlich zur Identifizierung einsetzen würde.[249] Der EuGH hat diesen Ansatz in der Sache Breyer für dynamische IP-Adressen entwickelt: Solche Adressen sind für den Diensteanbieter nur dann personenbezogen, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die Person anhand des bei einem Dritten vorhandenen Zusatzwissens bestimmen zu lassen.[250]

Diese Betrachtung aus der Perspektive des die Daten verarbeitenden Akteurs hat der Gerichtshof in der Sache EDSB/SRB ausdrücklich verallgemeinert und damit auch für den hier interessierenden Zusammenhang bestätigt: Pseudonymisierte – und erst recht verschlüsselte – Daten müssen „nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden". Die Pseudonymisierung kann andere Personen als den Verantwortlichen je nach den Umständen tatsächlich an einer Identifizierung hindern, sodass die betroffene Person für sie nicht oder nicht mehr identifizierbar ist.[251] Der Einsatz eines Mittels gilt dabei nach allgemeinem

[249] Vgl. zur Gegenüberstellung von relativer und absoluter Theorie und zum Vorzug der relativen Betrachtung Auernhammer/*Eßer*, Art. 4 DSGVO, Rn. 20.

[250] EuGH, Urteil vom 19.10.2016, Breyer, C-582/14, Rn. 44, 49; bestätigt für die DSGVO durch EuGH, Mircom, C-597/19, Rn. 102.

[251] EuGH, Urteil vom 04.09.2025, EDSB/SRB, C-413/23 P, Rn. 85 f.

Ermessen als nicht wahrscheinlich, wenn das Identifizierungsrisiko de facto unbedeutend erscheint, etwa weil die Identifizierung praktisch nicht durchführbar wäre oder gesetzlich verboten ist.[252] Dieselbe Linie liegt dem – derzeit zur öffentlichen Konsultation gestellten – Entwurf der EDSA-Leitlinien 02/2026 zur Anonymisierung zugrunde, der die Anonymität aus der Perspektive jeder relevanten Stelle beurteilt und dabei auch Mittel einbezieht, die einer Stelle erst über Dritte zugänglich werden.

1.3.2. Übertragung auf die Datenarten und Rollen in ZaPuK

Für die Beurteilung der Anwendbarkeit ist innerhalb von ZaPuK zwischen Inhaltsdaten und Kommunikationsmetadaten sowie zwischen den Akteuren zu unterscheiden, die Zugriff auf den Klartext haben, und jenen, denen nur das Chiffrat vorliegt.

a) Inhaltsdaten unter Ende-zu-Ende-Verschlüsselung

Die Nachrichteninhalte werden nach den Grundentscheidungen der Zielarchitektur durchgängig Ende-zu-Ende-verschlüsselt transportiert und ausschließlich als Chiffrat gespeichert (ADR-0011, ADR-0012); der Klartext liegt bei der Einzelnutzer-Kommunikation allein im Endgerät (ADR-1100). Für einen Akteur, der lediglich das Chiffrat verarbeitet und die zur Entschlüsselung erforderlichen Schlüssel weder besitzt noch mit nach allgemeinem Ermessen wahrscheinlichen Mitteln erlangen kann, fehlt es hinsichtlich der Inhalte am Personenbezug. Die Verarbeitung der verschlüsselten Inhalte durch diese Akteure unterfällt insoweit nicht der DSGVO. Das entspricht der herrschenden Einordnung verschlüsselter Daten in der Literatur: Bei starker Verschlüsselung liegt gegenüber einer Stelle, die nicht über die Schlüssel verfügt und sich diese auch nicht verschaffen kann, keine Offenlegung personenbezogener Daten vor; das Datenschutzrecht gilt für deren Einbringung in die fremde Infrastruktur dann nicht.[253] Eine wirksame

[252] EuGH a.a.O. Rn. 82; vgl. bereits Breyer, C-582/14, Rn. 46.
[253] Freund, in: Schuster/Grützmacher, IT-Recht, 2. Aufl., Art. 44 DSGVO, Rz. 29; zur Wirkungsweise der Verschlüsselung als Beschränkung der Lesbarkeit auf die Schlüsselinhaber Kramer/Meints, in: Auernhammer, 8. Aufl., Art. 32 DSGVO, Rn. 28.

Ende-zu-Ende-Verschlüsselung führt dazu, dass weder der Diensteanbieter noch ein sonstiger Dritter Zugriff auf die Kommunikationsinhalte erhält.[254]

Konkret bedeutet dies für die Kerninfrastruktur: Das Postfach-Backend einschließlich Homeserver und Content-Repository (ADR-1103), der die Bereitstellungsbestätigung erzeugende Application Service (ADR-0018) und der Protokollkonverter (ADR-0010) verarbeiten hinsichtlich der Nachrichteninhalte keine personenbezogenen Daten, solange die Ende-zu-Ende-Verschlüsselung strikt gewahrt bleibt. Der Application Service bildet lediglich eine Prüfsumme über das Chiffrat und benötigt keinen Klartextzugriff; der Protokollkonverter transportiert verschlüsselte Container über die Systemgrenze, ohne die Verschlüsselungsschicht aufzubrechen. Für diese Akteure ist die DSGVO in Bezug auf die Inhaltsebene nicht einschlägig.

Diese Einordnung steht allerdings unter mehreren wichtigen Vorbehalten. Erstens ist Verschlüsselung ihrem Wesen nach umkehrbar und keine Anonymisierung; der Entwurf des EDSA zu den Leitlinien 02/2026 (zur Anonymisierung) betont zu Recht, dass Verschlüsselung eine Anonymisierung unterstützen, sie aber nicht ersetzen kann. Der fehlende Personenbezug beruht deshalb nicht auf einer endgültigen Beseitigung des Personenbezugs, sondern allein darauf, dass dem konkreten Akteur die Reidentifizierung nicht mit wahrscheinlichen Mitteln möglich ist. Zweitens ist diese Bewertung fortlaufend und im Zeitverlauf zu überprüfen, weil sich die verfügbare Technik und damit die „nach allgemeinem Ermessen wahrscheinlichen Mittel" ändern können; dem trägt das Prinzip der Krypto-Agilität Rechnung. Drittens – und für ZaPuK zentral – setzt der fehlende Personenbezug voraus, dass der Betreiber die Schlüssel *lückenlos* nicht erlangen kann. Sobald ein Akteur über einen Weg verfügt, den Schlüssel mit vertretbarem Aufwand zu erlangen, etwa über ein unzureichend gegen Betreiberzugriff abgesichertes serverseitiges Schlüssel-Backup oder über kollusives Zusammenwirken, wird das Chiffrat für ihn zu personenbezogenen Daten. Die Ausgestaltung der Schlüsselwiederherstellung (clientseitige Verschlüsselung des Key-Backups vor Ablage auf dem Homeserver) ist daher nicht nur ein Sicherheitsthema, sondern wirkt sich zugleich auf die (Nicht-)Anwendbarkeit des Datenschutzrecht aus.

[254] Klein, in: Moos, Datenschutz- und Datennutzung, 4. Aufl., M 28, Rz. 27.

b) Serverseitige Entschlüsselungsendpunkte

Anders liegt es, wo die Zielarchitektur bewusst einen Klartextzugriff im Machtbereich einer Organisation vorsieht. Bei Mehrbenutzer-Szenarien kann ein technischer Nutzer als E2EE-Teilnehmer am Vorgangsraum teilnehmen und erhält dann Zugriff auf die entschlüsselten Inhalte (ADR-1101 Option B, ADR-1102); ebenso terminiert bei der – nur als begründete Ausnahme zugelassenen – Variante „E2EE bis Organisationsgrenze" die Verschlüsselung auf einem Server der Organisation (ADR-1101 Option C). In diesen Konstellationen liegen personenbezogene Daten vor; die DSGVO ist auf die dortige Verarbeitung uneingeschränkt anwendbar. Gleiches gilt für eine an einem solchen Endpunkt durchgeführte Malware-Prüfung des Klartextes (ADR-1130). Die Wahl der Betriebs- und Terminierungsvariante entscheidet damit unmittelbar darüber, ob und in welchem Umfang datenschutzrechtliche Pflichten den serverseitigen Komponenten einer Organisation zugewiesen sind.

c) Kommunikationsmetadaten und pseudonyme Adressen

Von den Inhaltsdaten strikt zu trennen sind die Kommunikationsmetadaten – insbesondere die adressierenden MXIDs, die Zuordnung von Absender und Empfänger, Zeitpunkte und Routing-Informationen –, die nach dem Matrix-Protokoll im Postfach-Backend zwangsläufig unverschlüsselt vorliegen (vgl. ADR-1105). Diese Metadaten sind für die Betreiber personenbezogen. Die für Privatpersonen vorgesehene bereichsspezifische, pseudonyme Adressierung beseitigt den Personenbezug nicht, sondern stellt eine Pseudonymisierung im Sinne des Art. 4 Nr. 5 DSGVO dar; pseudonymisierte Daten, die durch Heranziehung zusätzlicher Informationen einer Person zugeordnet werden können, sind nach ErwGr. 26 Satz 2 DSGVO Informationen über eine identifizierbare Person. Für das Backend, das die pseudonyme MXID im laufenden Betrieb den zugehörigen Kommunikationsvorgängen zuordnet und – im Antragskontext – aus der Identität ableitet, ist die Person mit nach allgemeinem Ermessen wahrscheinlichen Mitteln zumindest indirekt bestimmbar. Die Metadatenverarbeitung durch die Postfach-Backends unterfällt daher der DSGVO, und zwar unabhängig davon, dass die Inhalte für dieselben Betreiber anonym sind. Dies unterstreicht zugleich, warum die architektonischen Grundentscheidungen zur Metadatenminimierung, zur Betreibertrennung zwischen Bürger- und

Organisationsdomäne und zum Verbot der domänenübergreifenden Zusammenführung datenschutzrechtlich geboten sind (vgl. zur Metadatenreduktion und zum Betreiberausschluss 3.6.3): Sie erhöhen das Schutzniveau nicht auf der Inhalts-, sondern gerade auf der trotz E2EE weiterhin regulierten Metadatenebene.

Eine Präzisierung ist für die Organisationsdomäne veranlasst. Die Zielarchitektur ordnet die Teilnehmenden gruppenbezogen getrennten Backends zu und geht dabei davon aus, dass die Metadaten der Kommunikation juristischer Personen untereinander keine vergleichbaren Risiken begründen (Architekturkonzept, Abschnitt 4.2.1). Diese Annahme trägt nicht durchgängig. Zwar schützt das Datenschutzrecht nur natürliche Personen (ErwGr. 14 Satz 2 DSGVO). Freiberuflich und gewerblich tätige Einzelpersonen sind aber natürliche Personen und zugleich Unternehmen im Sinne des § 2 Abs. 5 Satz 4 OZG iVm § 3 Abs. 1 Satz 1 Nr. 6 Buchst. a Unternehmensbasisregistergesetz (UBRegG). Ihre Kommunikationsmetadaten sind ohne Weiteres personenbezogen. Bei Ein-Personen-Gesellschaften können die Angaben zur juristischen Person auf die dahinterstehende natürliche Person durchschlagen und deshalb ebenfalls personenbezogene Daten sein. Für die Metadatenverarbeitung im Organisations-Backend gilt insoweit nichts anderes als in der Bürgerdomäne. Die Trennung der Domänen verliert für diese Gruppe gleichwohl nicht ihren Wert; sie beruht lediglich auf einem anderen Grund. Sie hält die berufliche von der privaten Kommunikation derselben Person getrennt und entspricht damit einem eigenständigen Interesse der Betroffenen. Für die Adressbildung ist im Ergebnis nach hier vertretener Auffassung kein Sonderregime erforderlich. Zwar sind die sprechenden Adressbestandteile, die ADR-1104 für Funktionspostfächer vorsieht, bei Ein-Personen-Einheiten nicht personenbezugsfrei. Sie betreffen die dahinterstehende Person aber ausschließlich in ihrer beruflichen Sphäre, die nach allgemeinen Grundsätzen ein geringeres Schutzniveau beansprucht als die Privatsphäre; ein Geheimhaltungsinteresse setzt sich dort nur bei spezifischen Anhaltspunkten durch. Hinzu kommt, dass die berufliche Identität ohnehin offenzulegen ist, etwa nach § 5 Abs. 1 Nr. 1 Digitale-Dienste-Gesetz (DDG) sowie über die Register- und Kammerpublizität. Eine Ungleichbehandlung gegenüber den übrigen Organisationsadressen wäre daher nicht gerechtfertigt und würde die Adressierung ohne Schutzgewinn verkomplizieren.

d) Endgeräte und versendende Stellen

An den Endpunkten der Verschlüsselung – den Endgeräten der Nutzenden und den Fachverfahren der versendenden Stellen – liegt der Klartext vor. Für diese Akteure sind sowohl Inhalte als auch Metadaten personenbezogen; die DSGVO ist vollumfänglich anwendbar. Für die versendende Behörde oder Organisation folgt daraus insbesondere, dass sie sich der datenschutzrechtlichen Verantwortung nicht unter Hinweis darauf entziehen kann, dass die Nachricht auf dem Transportweg verschlüsselt und für die Backend-Betreiber anonym ist. Der EuGH hat in der Sache EDSB/SRB klargestellt, dass die Frage des Personenbezugs für die eine Stelle treffenden Pflichten aus deren eigener Perspektive zu beurteilen ist; wer selbst über den Klartext verfügt, bleibt an die DSGVO gebunden, auch wenn die Daten beim Empfänger oder beim Übermittler anonym sein mögen.[255] Für die architektonisch angelegte Übermittlung gilt zudem der aus der EuGH-Entscheidung Breyer und der Folgerechtsprechung abzuleitende Ketten-Gedanke: Reicht eine Stelle Daten an einen Empfänger weiter, der die Person mit wahrscheinlichen Mitteln bestimmen kann, spricht dies für einen Personenbezug bereits auf der Übermittlungsstufe. Dieser Gesichtspunkt trifft in ZaPuK die versendenden Stellen, nicht aber die reinen Chiffrat-Transporteure, denen der Schlüssel gerade fehlt.

1.3.3. Folgerungen für die Architektur von ZaPuK

Die Anwendbarkeit des Datenschutzrechts lässt sich für ZaPuK nicht einheitlich, sondern nur differenziert nach Akteur und Datenart beantworten. Die durchgängige Ende-zu-Ende-Verschlüsselung ist dabei nicht nur eine Sicherheitsmaßnahme, sondern zugleich ein anwendbarkeitsbegrenzendes Gestaltungsmittel, das den Kreis der datenschutzrechtlich verantwortlichen Stellen auf der Inhaltsebene deutlich verengt. Für die Architektur ist daraus Folgendes abzuleiten:

- Die Grundentscheidung für eine strikte, ausschließlich an den Endpunkten terminierende Ende-zu-Ende-Verschlüsselung (ADR-0011, ADR-0012, ADR-1100) wird bestärkt. Sie bewirkt, dass die Backend-Betreiber, der Application Service und der

[255] Vgl. EuGH, C-413/23 P, Rn. 84 f. zur Maßgeblichkeit der Verantwortlichenperspektive.

Protokollkonverter hinsichtlich der Inhalte keine personenbezogenen Daten verarbeiten und insoweit nicht den Pflichten der DSGVO unterliegen.

- Der fehlende Personenbezug der Inhalte steht und fällt mit der lückenlosen Unmöglichkeit des Schlüsselzugriffs durch die Betreiber. Das Schlüsselmanagement, insbesondere ein serverseitiges Key-Backup, ist deshalb so auszugestalten, dass der Betreiber die Schlüssel auch nicht mit vertretbarem Aufwand erlangen kann (clientseitige Verschlüsselung vor Ablage, wie im Architekturkonzept, Abschnitt 5.4.13, vorgesehen). Dies sollte ergänzend in den Anschlussbedingungen abgesichert werden.

- Für die serverseitigen Entschlüsselungsvarianten (technischer Nutzer als E2EE-Teilnehmer, Terminierung an der Organisationsgrenze, serverseitige Malware-Prüfung) ist von voller Anwendbarkeit der DSGVO im Machtbereich der jeweiligen Organisation auszugehen. Die Zulassung dieser Varianten als Ausnahme mit Begründungs- und Dokumentationspflicht (ADR-1101) ist folgerichtig und aus datenschutzrechtlicher Sicht beizubehalten.

- Die Kommunikationsmetadaten bleiben trotz pseudonymer Adressierung personenbezogen. Die Verarbeitung durch die Postfach-Backends unterliegt daher der DSGVO. Die architektonischen Maßnahmen zur Metadatenminimierung, zur Betreibertrennung und zum Ausschluss domänenübergreifender Verknüpfung sind maßgebliche Mittel zur Risikobegrenzung auf dieser weiterhin regulierten Ebene.

- Bei Freiberuflern, Einzelunternehmern und Ein-Personen-Gesellschaften sind auch die Metadaten der Organisationsdomäne personenbezogen; die Maßnahmen zur Metadatenminimierung sind dort entsprechend anzuwenden. Die Trennung der Domänen rechtfertigt sich für diese Gruppe nicht aus einem geringeren Schutzbedarf, sondern daraus, dass sie berufliche und private Kommunikation derselben Person auseinanderhält. Für die Adressbildung bedarf es keiner Sonderregel: Sprechende Adressen von Funktionspostfächern (ADR-1104) betreffen die Person allein in ihrer beruflichen Sphäre und können mit den übrigen Organisationsadressen gleich behandelt werden.

- Weil Verschlüsselung keine Anonymisierung ist und die „wahrscheinlichen Mittel" technologieabhängig sind, ist die Einordnung fortlaufend zu überprüfen. Das Prinzip der Krypto-Agilität sollte um eine regelmäßige Neubewertung des Reidentifizierungsrisikos ergänzt werden; der EDSA-Entwurf 02/2026 empfiehlt eine solche periodische Reassessment-Praxis ausdrücklich.

- Die versendenden Stellen bleiben als Inhaber des Klartextes unabhängig von der Transportverschlüsselung uneingeschränkt datenschutzrechtlich verantwortlich. Verbindliche Vorgaben hierzu sollten über die Anschlussbedingungen etabliert werden, ohne die eigenständige Verantwortlichkeit der jeweiligen Stelle zu verlagern.

2. Datenschutzrechtliche Rollen

Kurzzusammenfassung. Die DSGVO knüpft ihre Pflichten an Rollen: Für jede Verarbeitung gibt es mindestens einen Verantwortlichen (Art. 4 Nr. 7 DSGVO), der über Zwecke und Mittel entscheidet; wirken mehrere Stellen an derselben Verarbeitung zusammen, kommt eine gemeinsame Verantwortlichkeit (Art. 26 DSGVO) in Betracht, und die weisungsgebundene Verarbeitung für einen anderen ist Auftragsverarbeitung (Art. 28 DSGVO). Verantwortlicher wird eine Stelle entweder durch eigene Zwecksetzung oder durch – auch implizite – Benennung im Recht; für Behörden ist die implizite Zuweisung über die Aufgabenzuweisung der Regelfall.

Für ZaPuK lässt sich die Verantwortlichkeit nicht einheitlich, sondern nur rollen- und verarbeitungsbezogen bestimmen. Feststeht, dass jeder Backend-Betreiber für die von ihm verarbeiteten Daten – insbesondere die trotz Ende-zu-Ende-Verschlüsselung anfallenden Metadaten – datenschutzrechtlich verantwortlich ist und dass die versendenden Stellen als Inhaber des Klartexts uneingeschränkt verantwortlich bleiben. Offen und nicht eindeutig zu beantworten ist dagegen, ob im verteilten Mehr-Betreiber-Betrieb neben getrennten Verantwortlichkeiten zugleich eine gemeinsame Verantwortlichkeit entsteht (siehe 2.2). Es wird empfohlen, die Verantwortlichkeit – dem Vorbild des § 8a Abs. 4 OZG folgend – spezialgesetzlich klarzustellen.

2.1. Die datenschutzrechtlichen Rollen der DSGVO

Datenschutzrechtliche Pflichten treffen stets einen Verantwortlichen, bezogen auf einen konkreten Verarbeitungsvorgang. Die Bestimmung der Rollen erfolgt daher in zwei Schritten: Zunächst ist zu klären, welche Verarbeitung in Rede steht und ob sie – nach dem in Abschnitt 1.3 entwickelten relativen Maßstab – überhaupt personenbezogene Daten betrifft; erst dann ist zu fragen, wer für sie verantwortlich ist. Dieser rollen- und vorgangsbezogene Zuschnitt ist für eine verteilte Infrastruktur wie ZaPuK von grundlegender Bedeutung, weil sich dieselbe Stelle für einen Verarbeitungsschritt als Verantwortliche, für einen anderen als Auftragsverarbeiterin und für einen dritten – mangels Personenbezugs der ihr vorliegenden Daten – außerhalb des Anwendungsbereichs der DSGVO bewegen kann.

2.1.1. Der Verantwortliche und die Wege zur Verantwortlichkeit

Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet. Der Begriff ist weit auszulegen, damit für jede Verarbeitung mindestens ein Adressat für die Rechte der betroffenen Personen zur Verfügung steht; er setzt weder eigene Rechtspersönlichkeit noch einen tatsächlichen Zugriff auf die Daten voraus. So kann nach der Rechtsprechung des EuGH auch eine organisatorisch unselbständige Stelle Verantwortliche sein, sofern sie über Zwecke und Mittel entscheidet.[256]

Zum Verantwortlichen wird eine Stelle auf zwei Wegen. Sie kann die Zwecke und Mittel der Verarbeitung aus Eigeninteresse selbst festlegen. Sie kann aber auch durch Rechtsvorschrift als Verantwortliche benannt werden, wenn Zwecke und Mittel der Verarbeitung rechtlich vorgegeben sind (Art. 4 Nr. 7 Halbsatz 2 DSGVO); diese Benennung kann ausdrücklich oder – praktisch häufiger – implizit erfolgen. Für den öffentlichen Bereich ist anerkannt, dass die gesetzliche Zuweisung einer Aufgabe im Zweifel zugleich die Zuweisung der Verantwortlichkeit für die zur Aufgabenerfüllung erforderliche Datenverarbeitung enthält; wo das Recht Zweck und Mittel der Verarbeitung vorgibt und einer Stelle die Aufgabe zuweist, ist regelmäßig diese Stelle Verantwortliche.[257] Diese Wertung liegt auch der jüngeren EuGH-Rechtsprechung zugrunde,

[256] EuGH, Urteil vom 27.02.2025, C-638/23 – Amt der Tiroler Landesregierung.
[257] Vgl. Eßer, in: Auernhammer, DSGVO/BDSG, 8. Aufl. 2024, Art. 4, Rn. 79.

wonach das nationale Recht die Zwecke und Mittel einer Verarbeitung vorgeben und den Verantwortlichen bestimmen darf.[258] Der nationale Gesetzgeber knüpft hieran über die Öffnungsklausel des Art. 6 Abs. 3 DSGVO an (s.o. 1.2).

2.1.2. Gemeinsame Verantwortlichkeit

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel einer Verarbeitung fest, sind sie gemeinsam Verantwortliche und haben in einer transparenten Vereinbarung festzulegen, wer welche Pflichten erfüllt (Art. 26 Abs. 1 DSGVO). Die Rechtsprechung des EuGH hat die Voraussetzungen weit, zugleich aber unscharf konturiert. Erforderlich ist zwar, dass jeder Beteiligte für sich die Merkmale des Art. 4 Nr. 7 DSGVO erfüllt; es genügt aber, dass eine Stelle zu eigenen Zwecken auf die Verarbeitung Einfluss nimmt, und es ist nicht erforderlich, dass jeder Beteiligte Zugang zu den Daten hat.[259] Aus der gemeinsamen Verantwortlichkeit folgt zudem keine gleichwertige Verantwortlichkeit; der Grad der Verantwortung ist für jede Phase gesondert nach den Umständen des Einzelfalls zu beurteilen. Notwendige Voraussetzung bleibt allerdings eine gemeinsame Festlegung, die sich sowohl auf den Zweck als auch auf die Mittel bezieht; die bloße Nutzung einer gemeinsamen Infrastruktur begründet für sich noch keine gemeinsame Verantwortlichkeit, wenn die jeweiligen Verarbeitungen voneinander abtrennbar sind und ohne Zutun der anderen Seite erfolgen könnten.[260]

Eine gemeinsame Verantwortlichkeit kann nach der Rechtsprechung auch durch nationales Recht begründet werden: Gibt das Recht bei einer Kette von Verarbeitungen, die dieselben Daten betreffen, die Zwecke und Mittel sämtlicher aufeinanderfolgender Verarbeitungen vor, kann es die beteiligten Stellen gemeinsam verantwortlich machen, sofern die Verarbeitungen durch die vorgegebenen Zwecke und Mittel verbunden sind und das Recht die jeweiligen Pflichten festlegt.[261] Diese Verbindung kann sich auch mittelbar aus dem Recht ergeben, sofern sie sich den einschlägigen Vorschriften hinreichend deutlich entnehmen lässt.[262] Umgekehrt

[258] EuGH, C-231/22 – État belge, Rn. 44.
[259] EuGH, C-683/21 – Nacionalinis visuomenės sveikatos centras, Rn. 40 ff.; C-604/22 – IAB Europe, Rn. 58; C-231/22 – État belge, Rn. 48.
[260] Freund, in: Schuster/Grützmacher, IT-Recht, 2. Aufl. 2025, Art. 26 DSGVO, Rz. 21, 30.
[261] EuGH, C-231/22 – État belge, Rn. 45, 49.
[262] EuGH, a.a.O., Rn. 50.

bleibt es, wo eine solche Verbindung fehlt, bei einer getrennten Verantwortlichkeit: Bei einer mehrstufigen Vorgangskette kann insofern ein schlichter Übergabepunkt bestehen, an dem Daten von einer verantwortlichen Stelle an die nächste übermittelt werden, ohne dass eine gemeinsame Verantwortlichkeit entsteht.

2.1.3. Abgrenzung zur Auftragsverarbeitung

Von der Verantwortlichkeit zu unterscheiden ist die Auftragsverarbeitung.[263] Auftragsverarbeiter ist, wer personenbezogene Daten weisungsgebunden für den Verantwortlichen verarbeitet, ohne über Zwecke und wesentliche Mittel zu entscheiden (Art. 4 Nr. 8, Art. 28 DSGVO). Kennzeichnend ist ein Über-/Unterordnungsverhältnis, in dem der Verantwortliche dem Auftragsverarbeiter verbindliche Weisungen erteilen kann; dieses muss rechtlich und tatsächlich begründbar sein. Für IT-Dienstleistungen – insbesondere Hosting, Wartung und Betrieb – ist die Auftragsverarbeitung der Regelfall; sie ist auch zwischen öffentlichen Stellen und selbst innerhalb desselben öffentlich-rechtlichen Rechtsträgers möglich und kann statt durch Vertrag auch durch ein „anderes Rechtsinstrument" im Sinne des Art. 28 Abs. 3 DSGVO (etwa durch Rechtsverordnung, Verwaltungsvorschrift oder Satzung) begründet werden. Maßgeblich ist stets die tatsächliche Ausgestaltung: Ist eine Stelle kraft eigener Rechtsgrundlage zur Aufgabenerfüllung berufen, verarbeitet sie nicht weisungsgebunden, sondern in eigener Verantwortung; ein gleichwohl „vorsorglich" geschlossener Auftragsverarbeitungsvertrag ginge dann an der Rechtslage vorbei.

2.2. Übertragung auf die verteilte Architektur von ZaPuK

ZaPuK ist eine föderierte Mehr-Betreiber-Infrastruktur: Nachrichten werden in Postfach-Backends verschlüsselt gespeichert, die untereinander föderieren; zentrale Backends je Teilnehmergruppe (Privatpersonen, private Organisationen, öffentliche Stellen, Justiz) stehen neben dezentral betriebenen Backends und weiteren Komponenten wie Self-Service-Portal,

[263] Die Ausführung in diesem Abschnitt orientieren sich an der ausführlichen Aufarbeitung im Gutachten des Kompetenzteams Datenschutz (Hamburg) zur datenschutzrechtlichen Verantwortlichkeit bei zentraler Bereitstellung von IKT-Diensten, das für die föderale Verwaltungsdigitalisierung als Referenz herangezogen werden kann.

Adressregister, Raum-Management-Service und Nachweisstellen (vgl. ADR-1103, ADR-1104, ADR-1111). Vor diesem Hintergrund lässt sich die datenschutzrechtliche Verantwortung nicht pauschal, sondern nur differenziert nach Rolle, Komponente und Verarbeitungsschritt bestimmen.

2.2.1. Ausgangspunkt: Was ist personenbezogen?

Aus der Anwendbarkeitsanalyse (1.3) folgt, dass die Backend-Betreiber hinsichtlich der Nachrichteninhalte, die ihnen nur als Chiffrat vorliegen und deren Schlüssel sie nicht erlangen können, keine personenbezogenen Daten verarbeiten. Insoweit stellt sich die Frage der Verantwortlichkeit nicht. Sie stellt sich aber uneingeschränkt auf zwei Ebenen: erstens bei den Kommunikationsmetadaten, die im Postfach-Backend zwangsläufig unverschlüsselt anfallen und trotz pseudonymer Adressierung für die Betreiber personenbezogen bleiben; zweitens überall dort, wo Klartext anfällt – an den Endgeräten, bei den versendenden Stellen und an serverseitigen Entschlüsselungsendpunkten (technischer Nutzer, Organisationsgrenze). Die datenschutzrechtliche Rollenverteilung ist daher vor allem eine Frage der Metadaten- und der Klartextebene.

2.2.2. Rollen der einzelnen Akteure

a) Versendende und empfangende Stellen

Die Behörden, Organisationen und Privatpersonen, die als Inhaber des Klartexts kommunizieren, entscheiden über Zwecke und Mittel der inhaltlichen Verarbeitung und sind hierfür jeweils selbst Verantwortliche. Für die öffentlichen Stellen ergibt sich die Verantwortlichkeit regelmäßig implizit aus der fachgesetzlichen Aufgabenzuweisung in Verbindung mit dem jeweils anwendbaren Datenschutzregime (BDSG, Landesrecht, bereichsspezifisches Recht). Diese Verantwortung besteht unberührt dessen, dass die Nachricht auf dem Transportweg verschlüsselt und für die Backend-Betreiber anonym ist.

b) Backend-Betreiber

Die Betreiber der Postfach-Backends verarbeiten die Kommunikationsmetadaten und sind hierfür datenschutzrechtlich verantwortlich. Beim souveränen Betrieb (ADR-1103, Option C) betreibt die Organisation ihr Backend selbst und ist für die dort anfallende Verarbeitung eigenständig verantwortlich. Bei Nutzung eines zentral betriebenen Backends (Optionen A und B) verarbeitet der zentrale Betreiber Metadaten, die den teilnehmenden Organisationen und ihren Kommunikationsvorgängen zuzuordnen sind. Hier ist die Rolle des Betreibers gerade nicht eindeutig vorgezeichnet (dazu sogleich).

2.2.3. Raum-Management-Service und technische Nutzer

Betreibt eine Organisation zur Umsetzung von Funktionspostfächern einen Raum-Management-Service mit technischem Nutzer (ADR-1101 Option B, ADR-1102), und nimmt dieser als E2EE-Teilnehmer am Vorgangsraum teil, liegt Klartextzugriff im Machtbereich der Organisation vor; die dortige Verarbeitung unterfällt uneingeschränkt der DSGVO und ist der Organisation als Verantwortlicher zuzurechnen. Lässt die Organisation diese Komponenten durch einen IT-Dienstleister betreiben, ist dies regelmäßig als Auftragsverarbeitung auszugestalten (so ausdrücklich ADR-1101, ADR-1103); die datenschutzrechtliche Verantwortung verbleibt bei der Organisation.

2.2.4. Zentrale Querschnittskomponenten

Für Self-Service-Portal, Adressregister und Nachweisstellen ist gesondert zu prüfen, wer über Zwecke und Mittel entscheidet. Soweit diese Dienste eine eigenständige, gesetzlich zugewiesene Funktion erfüllen (etwa die Führung des Adressregisters), spricht dies für eine eigene Verantwortlichkeit der betreibenden Stelle; soweit sie lediglich unterstützend im Auftrag der teilnehmenden Stellen tätig werden, kommt Auftragsverarbeitung in Betracht.

2.2.5. Verantwortlichkeit im verteilten Betrieb

a) Verarbeitung der Metadaten durch die Backend-Betreiber

Für die Verarbeitung der Metadaten durch die zentralen Backend-Betreiber und für das Zusammenwirken mehrerer Betreiber im föderierten Verbund lässt sich die Rolle nicht rechtssicher aus den allgemeinen Kriterien ableiten. Drei Einordnungen sind denkbar, die sich nicht wechselseitig ausschließen, sondern je nach Verarbeitungsschritt nebeneinander treten können.

Nahe liegt zunächst eine getrennte Verantwortlichkeit in einer Kette: Jeder Backend-Betreiber verantwortet die Verarbeitung in seiner Sphäre, die Übermittlung an das nächste Backend bildet einen Übergabepunkt, und die versendende bzw. empfangende Stelle verantwortet die Inhaltsebene. Dieses Modell entspricht der Grundwertung des § 8a Abs. 4 OZG, der für den länderübergreifenden Onlinedienst ausdrücklich eine Kette getrennter Verantwortlichkeiten anordnet: Verantwortlich für die Verarbeitung im Onlinedienst ist ausschließlich die betreibende Behörde, während die Verantwortlichkeit der empfangenden Fachbehörde unberührt bleibt. Angesichts der stark dezentral angelegten ZaPuK-Struktur spricht hierfür zusätzlich, dass es an einer zentralen Instanz fehlt, die den „Betrieb der Plattform" insgesamt verantwortet; wo eine solche zentrale Bündelung fehlt, deutet der Vergleich mit den Plattform-Konstellationen eher auf getrennte Verantwortlichkeiten hin.

Nicht ganz ausgeschlossen erscheint gleichwohl eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO. Sie setzt eine gemeinsame Festlegung von Zwecken und Mitteln oder eine hinreichend deutliche „Verbindung" der Verarbeitungen voraus. Eine solche Verbindung könnte sich aus der gemeinsamen, aufeinander abgestimmten Ausgestaltung des Verbunds ergeben – etwa aus einheitlichen Anschlussbedingungen, gemeinsam getragenen technischen Standards und einer übergreifenden Governance. Da der EuGH weder einen Datenzugriff noch einen gleichrangigen Einfluss verlangt und eine gemeinsame Verantwortlichkeit auch durch – mittelbares – nationales Recht begründet werden kann,[264] lässt sich eine gemeinsame

[264] EuGH, C-231/22 – État belge, Rn. 48 ff.

Verantwortlichkeit bei entsprechender rechtlicher oder tatsächlicher Verknüpfung jedenfalls nicht sicher verneinen.

b) Weisungsgebundener Betrieb als Auftragsverarbeitung

Für die Metadatenverarbeitung durch die zentralen Betreiber im Verhältnis zu den teilnehmenden Stellen kommt schließlich eine Auftragsverarbeitung in Betracht, wenn und soweit der Betrieb weisungsgebunden im Interesse der teilnehmenden Stellen erfolgt und deren Weisungsbefugnis rechtlich und tatsächlich begründet werden kann. Dieses Modell stößt für die föderierte Kerninfrastruktur allerdings an Grenzen, weil ein einzelner Betreiber vielen Verantwortlichen zugleich dient und wesentliche Mittel – Protokollwahl, Verschlüsselungsarchitektur, Metadatentrennung – nicht zur Disposition der einzelnen teilnehmenden Stelle stehen. Für abgegrenzte Unterstützungsleistungen im Machtbereich einer Organisation (Option B) bleibt die Auftragsverarbeitung dagegen der sachgerechte Rahmen.

c) Ergebnis

Im Ergebnis lässt sich die Frage nach der Verantwortung im verteilten Betrieb nach geltendem Recht nicht eindeutig beantworten; die Einordnung hängt von der konkreten Ausgestaltung des Verbunds ab und ist für jeden Verarbeitungsvorgang gesondert zu beurteilen. Diese Rechtsunsicherheit ist nicht auf ZaPuK beschränkt, sondern ein bekanntes Strukturproblem verteilter Verwaltungsinfrastrukturen. Der Gesetzgeber hat hierauf für die Verwaltungsdigitalisierung bereits mehrfach mit ausdrücklichen Zuweisungen reagiert – neben § 8a Abs. 4 OZG etwa in einzelnen Landesregelungen. Diese Regelungstechnik empfiehlt sich auch für ZaPuK.

2.2.6. Absicherung der Metadatentrennung

Die datenschutzrechtliche Rollenzuordnung ist nicht nur eine Frage der Zurechnung, sondern auch ein Instrument des Betreiberausschlusses (siehe 3.6.3). Die architektonische Trennung der Metadatenbestände zwischen Bürger- und Organisationsdomäne verliert ihren Schutzwert, wenn ein einziges Rechtssubjekt rechtlich und technisch in der Lage wäre, beide Bestände zusammenzuführen. Die Verantwortlichkeitsstruktur sollte daher so gewählt werden, dass sie eine domänenübergreifende Zusammenführung gerade nicht ermöglicht, sondern absichert – etwa

durch getrennte Betreiber mit ausdrücklichem Zusammenführungs- und Querzugriffsverbot. Zur rechtlichen Grundlage (getrennte Verantwortlichkeit, Auftragsverarbeitung mit Weisungsbindung oder spezialgesetzliche Zuweisung) siehe 3.6.3. Datenschutzrechtlich tragen sowohl Art. 5, 25 und 32 DSGVO als auch das telekommunikationsbezogene Datenschutzrecht (§ 3 TDDDG) das Ziel der Nichtverkettung.

2.3. Folgerungen für die Architektur von ZaPuK

Für die ZaPuK-Architektur ergibt sich aus dem Vorstehenden:

- Die Entscheidung, ZaPuK als domänenagnostische Infrastruktur ohne fachspezifische Logik auszugestalten (ADR-0001), ist aus Sicht der datenschutzrechtlichen Rollenzuordnung folgerichtig: Welche Stelle für welche Verarbeitung verantwortlich ist, bestimmt sich nach dem jeweiligen Verarbeitungskontext und kann von der Infrastruktur nicht vorweggenommen werden. Die Architektur muss diese Zuordnung ermöglichen und dokumentierbar machen, ohne sie zu präjudizieren.

- Fest steht, dass jeder Backend-Betreiber für die von ihm verarbeiteten Metadaten und jede Stelle mit Klartextzugriff (Endgeräte, versendende Stellen, serverseitige Entschlüsselungsendpunkte) für die dortige Verarbeitung datenschutzrechtlich verantwortlich ist. Diese Verantwortung bleibt bestehen und kann durch die E2EE-Verschlüsselung beim Transport nicht ausgeschlossen werden.

- Ob im verteilten Betrieb neben getrennten Verantwortlichkeiten zugleich eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO entsteht, ist nach geltendem Recht nicht sicher zu beantworten. Es wird empfohlen, die Verantwortlichkeit – dem Vorbild des § 8a Abs. 4 OZG folgend – durch Rechtsvorschrift ausdrücklich zuzuweisen. Dies schafft Rechtssicherheit gegenüber der kasuistischen Beurteilung, kann eine gesonderte Vereinbarung nach Art. 26 Abs. 1 DSGVO entbehrlich machen und erlaubt es zugleich, die Verantwortlichkeit so zuzuschneiden, dass die Metadatentrennung zwischen den Domänen abgesichert wird (siehe 3.6.3).

- Wird der Betrieb einzelner Komponenten (insbesondere Raum-Management-Service und Berechtigungsverzeichnis im delegierten Betrieb nach ADR-1103 Option B) durch Dritte übernommen, ist dies als Auftragsverarbeitung nach Art. 28 DSGVO auszugestalten; für öffentliche Stellen kommt auch ein „anderes Rechtsinstrument" in Betracht. Die eigenständige Verantwortlichkeit der jeweiligen Organisation bleibt hiervon unberührt.

- Verbindliche Vorgaben gegenüber den teilnehmenden Stellen und Betreibern – insbesondere Zusammenführungs- und Querzugriffsverbote sowie technische Trennungsanforderungen – sind über die Anschlussbedingungen (ADR-1145) zu transportieren. Die datenschutzrechtliche Verantwortung der jeweiligen Stelle besteht jedoch unabhängig/unberührt davon.

3. Grundsätze des Datenschutzes

Die wesentlichen datenschutzrechtlichen Anforderungen an die Verarbeitung sind in Art. 5 DSGVO zusammengefasst: Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit, flankiert durch die Rechenschaftspflicht. Sie bilden den durchgängigen Bewertungsmaßstab für die Architektur von ZaPuK und werden in diesem Abschnitt erörtert. Zweckbindung und Datenminimierung prägen zudem bereits die Grundentscheidungen zur domänenagnostischen Ausgestaltung, zur Metadatenminimierung und zur pseudonymen Adressierung (siehe 1.2 und 1.3).

3.1. Rechtmäßigkeit

Kurzzusammenfassung. Der Grundsatz der Rechtmäßigkeit (Art. 5 Abs 1 lit. a DSGVO) verlangt für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dem Datenschutzrecht liegt damit ein grundsätzliches Verbot der Verarbeitung mit Erlaubnisvorbehalt zugrunde.

Für ZaPuK sind zwei Verarbeitungsebenen zu unterscheiden. Die fachliche Verarbeitung der Nachrichteninhalte liegt bei den kommunizierenden Stellen, die über den Klartext verfügen; ihre Rechtsgrundlage ergibt sich aus dem jeweiligen Fachrecht und wird von der domänenagnostischen Infrastruktur (ADR-0001) nicht bereitgestellt. Davon zu trennen ist die Verarbeitung

im Infrastrukturbetrieb – insbesondere der trotz Ende-zu-Ende-Verschlüsselung personenbezogenen Kommunikationsmetadaten durch die Backend-Betreiber –, die einer eigenen Rechtsgrundlage bedarf.

Für öffentliche Stellen kommen als Rechtsgrundlage Art. 6 Abs. 1 lit. c und lit. e DSGVO in Verbindung mit Art. 6 Abs. 2 und 3 DSGVO und dem nationalen Recht (§ 3 BDSG bzw. Landesrecht oder bereichsspezifisches Recht) in Betracht; ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f) scheidet für Behörden aus. Private Teilnehmer stützen sich auf Einwilligung, Vertrag oder berechtigtes Interesse. Da § 3 BDSG nur eine Auffang- und Reservenorm für Verarbeitungen geringer Eingriffsintensität ist, die massenhafte und potenziell hochsensible Metadatenverarbeitung im Verbund aber eingriffsintensiv ist, empfiehlt sich – dem Vorbild des § 8 OZG folgend – eine spezialgesetzliche Rechtsgrundlage (siehe 3.6.3 und 2.2). Der übergreifende Maßstab der Erforderlichkeit stützt die Grundentscheidungen für Ende-zu-Ende-Verschlüsselung, Metadatenminimierung und pseudonyme Adressierung.

3.1.1. Der Rechtmäßigkeitsgrundsatz und das Verbot mit Erlaubnisvorbehalt

Nach Art. 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Der Grundsatz der Rechtmäßigkeit wird durch Art. 6 DSGVO konkretisiert, der die Verarbeitung nur dann für rechtmäßig erklärt, wenn mindestens eine der dort genannten Bedingungen erfüllt ist. Das Datenschutzrecht folgt damit einem Verbot mit Erlaubnisvorbehalt: Jede Verarbeitung ist untersagt, sofern sie nicht durch eine der Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO – bei besonderen Kategorien zusätzlich durch einen Erlaubnistatbestand des Art. 9 Abs. 2 DSGVO – getragen wird. Neben der Rechtmäßigkeit im engeren Sinne verlangt Art. 5 Abs. 1 lit. a DSGVO zugleich eine faire und transparente Verarbeitung. Die daraus folgenden Informationspflichten treffen die jeweils verantwortliche Stelle und sind bei der Ausgestaltung der Nutzendenschnittstellen zu berücksichtigen.

Weil der Rechtmäßigkeitsgrundsatz an die konkrete Verarbeitung und die für sie verantwortliche Stelle anknüpft, lässt sich die Rechtmäßigkeit für ZaPuK nicht einheitlich, sondern nur rollen- und vorgangsbezogen beurteilen. Ob eine Verarbeitung überhaupt dem Datenschutzrecht

unterfällt, ist dabei nach dem in Abschnitt 1.1.3 entwickelten relativen Maßstab des Personenbezugs vorab zu klären. Erst wo personenbezogene Daten verarbeitet werden, stellt sich die Frage nach ihrer Rechtsgrundlage.

3.1.2. Zwei Ebenen der Verarbeitung: fachliche Verarbeitung und Infrastrukturbetrieb

Für die Frage der Rechtsgrundlage sind bei ZaPuK zwei Verarbeitungsebenen zu trennen, die unterschiedlichen Akteuren zugeordnet sind.

Auf der ersten Ebene steht die fachliche Verarbeitung der Nachrichteninhalte. Sie erfolgt bei den kommunizierenden Stellen – den versendenden und empfangenden Behörden, Organisationen und Privatpersonen –, die als Inhaber des Klartexts über Zwecke und Mittel der inhaltlichen Verarbeitung entscheiden. Diese Verarbeitung dient dem jeweiligen Fachverfahren und findet ihre Rechtsgrundlage im einschlägigen Fachrecht. Als domänenagnostische Kommunikationsinfrastruktur ohne fachspezifische Logik (ADR-0001) trifft ZaPuK insoweit keine eigene Aussage und stellt keine Rechtsgrundlage bereit; die Infrastruktur muss die fachlich getragene Verarbeitung lediglich ermöglichen. Aus der relativen Betrachtung des Personenbezugs (siehe 1.3) folgt zugleich, dass die reinen Transport- und Speicherakteure hinsichtlich der ihnen nur als Chiffrat vorliegenden Inhalte keine personenbezogenen Daten verarbeiten. Für sie stellt sich die Frage einer inhaltsbezogenen Rechtsgrundlage nicht.

Auf der zweiten Ebene steht die Verarbeitung im Infrastrukturbetrieb. Sie betrifft vor allem die im Postfach-Backend nach dem Matrix-Protokoll zwangsläufig unverschlüsselt anfallenden Kommunikationsmetadaten, die trotz pseudonymer Adressierung für die Betreiber personenbezogen bleiben (siehe 1.3), sowie die Verarbeitung an den serverseitigen Entschlüsselungsendpunkten (technischer Nutzer, Organisationsgrenze). Diese Verarbeitung bedarf einer eigenen, vom Fachrecht der kommunizierenden Stellen unabhängigen Rechtsgrundlage. Die nachfolgenden Ausführungen betreffen daher in erster Linie diese Infrastrukturebene sowie die Klartext-Endpunkte.

3.1.3. Rechtsgrundlagen der Beteiligten

Bei den privaten Teilnehmern – Privatpersonen und privaten Organisationen – kommen die allgemeinen Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO in Betracht, insbesondere die Einwilligung (lit. a), die Vertragserfüllung (lit. b) und das berechtigte Interesse (lit. f). Stützt sich die Verarbeitung auf eine datenschutzrechtliche Einwilligung, sind deren Wirksamkeitsvoraussetzungen nach Art. 6 Abs. 1 lit. a in Verbindung mit Art. 7 DSGVO zu wahren – insbesondere die Freiwilligkeit, die Nachweisbarkeit und die jederzeitige Widerrufbarkeit.

Bei den öffentlichen Stellen scheidet das berechtigte Interesse als Rechtsgrundlage aus; nach Art. 6 Abs. 1 UAbs. 2 DSGVO gilt lit. f nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Auch die Einwilligung scheidet als tragende Grundlage einer flächendeckenden Verwaltungskommunikation aus, da im Über-/Unterordnungsverhältnis gegenüber der Verwaltung die Freiwilligkeit der Einwilligung problematisch ist. Maßgebliche Rechtsgrundlagen sind vielmehr Art. 6 Abs. 1 lit. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) und lit. e DSGVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder Ausübung öffentlicher Gewalt). Beide Tatbestände sind nicht aus sich heraus tragfähig, sondern werden über die Öffnungsklauseln des Art. 6 Abs. 2 und Abs. 3 DSGVO durch das nationale Recht ausgefüllt. Als „vor die Klammer gezogene" Grundlage dient dabei § 3 BDSG für Bundesstellen und die entsprechenden Vorschriften der Landesdatenschutzgesetze für Landes- und Kommunalstellen; sie erklären die Verarbeitung für zulässig, soweit sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Vorrang genießen die bereichsspezifischen Rechtsgrundlagen (Abschnitt 1.2).

Von der datenschutzrechtlichen Einwilligung als Rechtsgrundlage der Verarbeitung ist die verwaltungsverfahrensrechtliche Einwilligung in die elektronische Bekanntgabe zu unterscheiden, auch wenn beide denselben Begriff verwenden. Wenn § 9 Abs. 1 OZG – ebenso wie § 41 Abs. 2a VwVfG und, allgemeiner, die Zugangseröffnung nach § 3a Abs. 1 VwVfG – die elektronische Bekanntgabe eines Verwaltungsakts von einer (bei § 9 OZG als erteilt geltenden) Einwilligung des Nutzers abhängig macht, betrifft dies nicht die Rechtmäßigkeit einer Datenverarbeitung, sondern die Eröffnung des elektronischen Zugangs und die daran anknüpfende

Bekanntgabewirkung. Diese Einwilligung wirkt auf der Seite der bekanntgebenden Behörde und ist Gegenstand des verwaltungsverfahrens- und zustellungsrechtlichen Teils (siehe D.II.1); sie ersetzt weder eine datenschutzrechtliche Rechtsgrundlage der beteiligten Stellen noch wird sie durch eine solche ersetzt. Für die datenschutzrechtliche Beurteilung der Rechtmäßigkeit bleibt es damit bei den Rechtsgrundlagen des Art. 6 DSGVO in Verbindung mit dem nationalen Recht.

3.1.4. Besondere Kategorien personenbezogener Daten

Über ZaPuK werden potenziell auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO übermittelt – etwa Gesundheits- oder Sozialdaten. Deren Verarbeitung ist grundsätzlich untersagt und nur bei Vorliegen eines Erlaubnistatbestands nach Art. 9 Abs. 2 DSGVO in Verbindung mit dem konkretisierenden nationalen Recht (für öffentliche Stellen insbesondere § 22 BDSG bzw. die landesrechtlichen Parallelvorschriften) zulässig. Für die Inhaltsebene wirkt sich dies bei den reinen Backend-Betreibern nicht aus, weil ihnen die Inhalte nur als Chiffrat vorliegen. Zu beachten ist jedoch, dass bereits Kommunikationsmetadaten den Charakter besonderer Kategorien annehmen können, wenn schon aus der Kommunikationsbeziehung selbst eine sensible Information hervorgeht – etwa die Kommunikation einer Privatperson mit einer bestimmten Facharztpraxis, aus der sich Rückschlüsse auf Gesundheitsdaten ziehen lassen (vgl. bereits Abschnitt zur Metadatenreduktion). Insoweit ist auf der weiterhin regulierten Metadatenebene die Zulässigkeit nach Art. 9 DSGVO gesondert zu prüfen.

Bedeutsam ist, dass § 22 Abs. 2 BDSG als Voraussetzung der Verarbeitung besonderer Kategorien angemessene und spezifische Schutzmaßnahmen verlangt und dabei ausdrücklich die Pseudonymisierung und die Verschlüsselung nennt. Die architekturprägenden Grundentscheidungen von ZaPuK – durchgängige Ende-zu-Ende-Verschlüsselung und pseudonyme, bereichsspezifische Adressierung – sind damit nicht nur Sicherheitsmaßnahmen, sondern zugleich rechtlich geforderte Garantien, die die Zulässigkeit einer Verarbeitung besonderer Kategorien überhaupt erst tragen. § 8 Abs. 9 OZG erstreckt die dortigen Verarbeitungsbefugnisse bereits auf besondere Kategorien und erklärt § 22 Abs. 2 BDSG für entsprechend anwendbar. Dies bestätigt die Regelungsbedürftigkeit auch für die Postfach- und Kommunikationsinfrastruktur.

3.1.5. Rechtsgrundlage für den Infrastrukturbetrieb: Auffangnorm oder spezialgesetzliche Grundlage

Für die Metadatenverarbeitung durch öffentliche Betreiber und für den Betrieb der zentralen Komponenten stellt sich die Frage, ob § 3 BDSG bzw. das jeweilige Landesrecht als Rechtsgrundlage ausreicht. § 3 BDSG ist zwar als allgemeine Befugnisnorm ausgestaltet, wirkt aber nur als Auffang- und Reservenorm. Fehlt eine konkrete und ausdrückliche fachgesetzliche Erlaubnis, kann auf ihn nur für Verarbeitungen mit geringer Eingriffsstärke zurückgegriffen werden. Bei höherer Eingriffsintensität ist eine spezialgesetzliche Grundlage erforderlich.[265] Die im ZaPuK-Verbund anfallende Verarbeitung ist der Sache nach eingriffsintensiv: Es handelt sich um die dauerhafte, massenhafte Verarbeitung von Kommunikationsmetadaten mit teils höchstem Schutzbedarf, deren Korrelation nach der eigenen Einschätzung der Zielarchitektur bis zu Risiken für die nationale Sicherheit reichen kann (vgl. Metadatenreduktion, 3.6.2). Für eine solche Verarbeitung trägt die allgemeine Auffangnorm allein nicht.

Der Gesetzgeber hat für die Verwaltungsdigitalisierung bereits eine passende Regelungstechnik entwickelt. § 8 OZG bildet die Rechtsgrundlage für die Datenverarbeitung im Nutzerkonto und erfasst über § 8 Abs. 5 Nr. 7 OZG ausdrücklich auch Kommunikationsinhaltsdaten, während § 8 Abs. 6 OZG die Verarbeitung von Dokumenten und Statusinformationen und § 8 Abs. 10 OZG die datenschutzrechtliche Verantwortlichkeit regelt. Da das Postfach nach § 2 Abs. 7 OZG Bestandteil des Nutzerkontos ist, erstreckt sich dieser Rahmen bereits auf die Postfachkommunikation der Bürgerseite. Für ZaPuK ist er allerdings nicht vollständig passend: Die Zielarchitektur geht über das Bürgerkonto hinaus, bezieht Organisationen und einen dezentralen Mehr-Betreiber-Betrieb ein und verortet die Verantwortlichkeit teils außerhalb der bisherigen Zuständigkeitszuweisung. Es empfiehlt sich daher, für die Infrastruktur- und Metadatenverarbeitung eine spezialgesetzliche Grundlage zu schaffen oder § 8 OZG entsprechend zu erweitern. Dies schafft Rechtssicherheit gegenüber der kasuistischen Beurteilung nach den Öffnungsklauseln und erlaubt es zugleich, Zweckbindung, Datenarten, Speicherdauer und Verantwortlichkeit ausdrücklich festzulegen. Diese Empfehlung steht in engem Zusammenhang mit der

[265] Eßer, in: Auernhammer, 8. Aufl. 2024, § 3 BDSG, Rn. 14.

Zuweisung der Verantwortlichkeit im verteilten Betrieb (2.2) und der Absicherung des Betreiberausschlusses (siehe 3.6.3) und wird dort vertieft.

3.1.6. Erforderlichkeit als übergreifender Maßstab

Alle behördlichen Rechtsgrundlagen stehen unter dem Vorbehalt der Erforderlichkeit. Diese ist im Staat-Bürger-Verhältnis mit Rücksicht auf Art. 7 und Art. 8 der EU-Grundrechtecharta nach dem Verhältnismäßigkeitsgrundsatz zu bestimmen. Erforderlich ist von mehreren geeigneten Maßnahmen diejenige, die die betroffene Person am wenigsten beeinträchtigt.[266] Der Europäische Gerichtshof stellt an die Annahme, ein milderes Mittel sei unzumutbar, hohe Anforderungen; insbesondere kann die mangelnde Zuweisung von Mitteln an eine Behörde es nicht rechtfertigen, auf eine aufwendigere, aber datenschonendere Verarbeitung zu verzichten.[267] Der Zweck der Erforderlichkeit liegt gerade im Verbot unnötiger Datenverarbeitungen und -ansammlungen, namentlich der Erhebung von Daten „auf Vorrat".[268]

Für die Architektur folgt daraus, dass die datensparsamen Grundentscheidungen von ZaPuK nicht nur zulässig, sondern rechtlich geboten sind. Die durchgängige Ende-zu-Ende-Verschlüsselung, die Metadatenminimierung, die pseudonyme Adressierung und der Verzicht auf zentrale Datenbestände (etwa auf ein Adressregister für Privatpersonen) verwirklichen das Erforderlichkeitsprinzip und die datenschonendste unter den geeigneten Ausgestaltungen. Sie sind zugleich der wirksamste Beitrag zur Rechtmäßigkeit, weil sie den Umfang der überhaupt personenbezogen verarbeiteten Daten von vornherein begrenzen.

3.1.7. Folgerungen für die Architektur von ZaPuK

Für die ZaPuK-Architektur ergibt sich aus dem Vorstehenden:

- Die Trennung zwischen der fachlich getragenen Verarbeitung der Inhalte und der Verarbeitung im Infrastrukturbetrieb ist konsequent beizubehalten. Die domänenagnostische Ausgestaltung (ADR-0001) ist folgerichtig: ZaPuK stellt für die fachliche

[266] Kramer, in: Auernhammer, 8. Auflage 2024, Art. 6 DSGVO, Rn. 63.
[267] Freund, in: Schuster/Grützmacher, IT-Recht, Art. 6 DSGVO, Rz. 38.
[268] Eßer, in: Auernhammer, 8. Auflage 2024, § 3 BDSG, Rn. 24.

Verarbeitung keine Rechtsgrundlage bereit, sondern ermöglicht sie; die jeweils kommunizierende Stelle bleibt für ihre Rechtsgrundlage verantwortlich.

- Für die Metadatenverarbeitung durch öffentliche Betreiber und den Betrieb der zentralen Komponenten reicht die Auffangnorm des § 3 BDSG angesichts der Eingriffsintensität nicht aus. Es wird empfohlen, eine spezialgesetzliche Rechtsgrundlage zu schaffen oder § 8 OZG zu erweitern und dabei Zweckbindung, Datenarten, Speicherdauer und Verantwortlichkeit ausdrücklich festzulegen (siehe 3.6.3 und 2.2).

- Die datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO) ist von der verwaltungsverfahrensrechtlichen Einwilligung in die elektronische Bekanntgabe (§ 9 Abs. 1 OZG, § 41 Abs. 2a VwVfG) zu unterscheiden. Letztere betrifft die Zugangseröffnung und Bekanntgabewirkung (siehe D.II.1).

- Die Verarbeitung besonderer Kategorien personenbezogener Daten ist – auch auf der Metadatenebene – gesondert nach Art. 9 DSGVO und § 22 BDSG zu beurteilen. Ende-zu-Ende-Verschlüsselung und Pseudonymisierung sind dabei rechtlich geforderte besondere Schutzmaßnahmen (§ 22 Abs. 2 BDSG) und werden dadurch gestützt.

- Der strenge Erforderlichkeitsmaßstab bestätigt die datensparsamen Grundentscheidungen (E2EE, Metadatenminimierung, pseudonyme Adressierung, Verzicht auf zentrale Register). Eine Verarbeitung „auf Vorrat" ist zu vermeiden; die Beschränkung auf das für den jeweiligen Zweck notwendige Maß ist über die Anschlussbedingungen (ADR-1145) verbindlich zu machen, ohne die eigenständige Verantwortlichkeit der teilnehmenden Stellen zu verlagern.

3.2. Zweckbindung

Kurzzusammenfassung. Der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) verlangt, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Er gilt als der zentrale Grundsatz des Datenschutzrechts, weil sich Erforderlichkeit, Angemessenheit und Speicherdauer jeder Verarbeitung erst an einem konkret festgelegten Zweck bemessen lassen.

Für ZaPuK sind – wie schon bei der Rechtmäßigkeit – zwei Ebenen zu trennen: die fachliche Verarbeitung der Nachrichteninhalte, deren Zweck das jeweilige Fachrecht der kommunizierenden Stelle festlegt und die die domänenagnostische Infrastruktur (ADR-0001) nicht bestimmt, und die Verarbeitung im Infrastrukturbetrieb, die eng an den Betriebszweck der sicheren, nachweisbaren Übermittlung zu binden ist. Praktisch entfaltet die Zweckbindung ihre wesentliche Wirkung auf der Metadatenebene: Für sie verlangen Art. 5 Abs. 1 lit. b DSGVO und – bei Einordnung als Telekommunikationsdienst – das Fernmeldegeheimnis (§ 3 Abs. 3 TDDDG) eine strikte Beschränkung auf den Diensterbringungszweck und ein Verbot der zweck- und domänenübergreifenden Weiterverwendung. Dieser Zweckbindung unmittelbar dienlich sind die architektonischen Grundentscheidungen zur Metadatentrennung, zum Betreiberausschluss (siehe 3.6.3) und zur bereichsspezifischen pseudonymen Adressierung (ADR-1105) sowie die Zweckbindung der bewusst erzeugten Nachweise (insbesondere der Bereitstellungsbestätigung, ADR-0018).

3.2.1. Zweckfestlegung und Weiterverarbeitungsverbot

Nach Art. 5 Abs. 1 lit. b DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Grundsatz enthält damit zwei Anforderungen. Er verlangt zunächst eine vorherige Festlegung des Verarbeitungszwecks – treffender als Zweckfestlegungsgrundsatz zu bezeichnen – und untersagt sodann die Weiterverarbeitung zu unvereinbaren Zwecken. Die Zweckfestlegung ist keine Förmelei, sondern Voraussetzung jeder weiteren datenschutzrechtlichen Prüfung: Ohne konkret bestimmten Zweck lassen sich weder die Erforderlichkeit noch die Angemessenheit noch die zulässige Speicherdauer beurteilen. Der festgelegte Zweck muss überdies hinreichend eng gefasst sein; eine zu allgemeine Zweckbeschreibung genügt der Vorgabe der Eindeutigkeit nicht. Ein nachträgliches „Nachschieben" eines bei der Erhebung nicht festgelegten Zwecks ist unzulässig.

Weil die betroffene Person auf eine spätere Verwendung ihrer Daten keinen unmittelbaren Einfluss mehr hat, bildet das Weiterverarbeitungsverbot den eigentlichen Schutzgehalt des Grundsatzes. Von diesem Verbot nimmt Art. 5 Abs. 1 lit. b DSGVO ausdrücklich die

Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für Forschungs- und für statistische Zwecke aus, sofern die Garantien des Art. 89 Abs. 1 DSGVO gewahrt sind. Diese Privilegierung ist für die Aufbewahrung und Archivierung der über ZaPuK abgewickelten Kommunikation von Bedeutung (siehe 3.5.1).

3.2.2. Zweckänderung und Weiterverarbeitung

Ob eine Weiterverarbeitung zu einem anderen als dem Erhebungszweck zulässig ist, beurteilt sich in erster Linie nach ihrer Vereinbarkeit mit dem ursprünglichen Zweck. Art. 6 Abs. 4 DSGVO nennt hierfür die maßgeblichen Kriterien, unter anderem die Verbindung zwischen ursprünglichem und beabsichtigtem Zweck, den Erhebungszusammenhang, die Art der Daten, die möglichen Folgen für die betroffenen Personen und – für ZaPuK besonders bedeutsam – das Vorhandensein geeigneter Garantien, wozu die Verschlüsselung und die Pseudonymisierung ausdrücklich zählen. Die architekturprägenden Grundentscheidungen von ZaPuK sind damit nicht nur Sicherheits-, sondern zugleich zweckbindungsrechtlich relevante Garantien.

Jenseits der Vereinbarkeit erlaubt das Recht eine Weiterverarbeitung zu anderen Zwecken nur auf gesonderter gesetzlicher Grundlage. Für öffentliche Stellen bestimmt § 23 BDSG (bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze) die eng gefassten Fälle einer zulässigen Zweckänderung, für nichtöffentliche Stellen § 24 BDSG. Soweit eine Verarbeitung dem JI-Regime unterfällt (Justiz-Backend, zweckabhängig), gilt der Grundsatz der Zweckbindung nach § 47 Nr. 2 BDSG und die Zweckänderung ist nur unter den engeren Voraussetzungen des § 49 BDSG zulässig. Die abstrakte Möglichkeit einer künftigen Nützlichkeit trägt eine Weiterverarbeitung in keinem dieser Regime; eine Verarbeitung „auf Vorrat" widerspricht gerade dem Zweckbindungsgrundsatz.

3.2.3. Bereichsspezifische Verschärfungen und das OZG als Vorbild

Für die von ZaPuK bereichsübergreifend zu ermöglichenden Kommunikationen treten teils erheblich strengere Zweckbindungsregime hinzu. Im Sozialdatenschutz bindet § 67c SGB X die Verarbeitung von Sozialdaten strikt an den Erhebungszweck und lässt eine anderweitige Verwendung nur in eng umgrenzten Fällen zu. Für ausschließlich zu Zwecken der

Datenschutzkontrolle, der Datensicherung oder des ordnungsgemäßen Betriebs gespeicherte Daten ordnet § 67c Abs. 5 SGB X eine besonders enge Zweckbindung an, die – parallel zur Behandlung der Logdaten – jede zweckfremde Auswertung ausschließt. Für die Steuerverwaltung verbietet das Steuergeheimnis (§ 30 AO) die unbefugte Offenbarung und Verwertung geschützter Daten und knüpft eine Weiterverwendung durch Empfänger ausdrücklich an den Offenbarungszweck (§ 30 Abs. 11 AO). Soweit ein Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (siehe V), begründet das Fernmeldegeheimnis die schärfste Ausprägung der Zweckbindung auf der Metadatenebene: Nach § 3 Abs. 3 TDDDG ist es den Verpflichteten untersagt, sich über das für die Diensterbringung erforderliche Maß hinaus Kenntnis von Inhalt oder näheren Umständen der Kommunikation zu verschaffen; erlangte Kenntnisse dürfen nur für diesen Zweck verwendet und nur weitergegeben werden, soweit ein Gesetz dies ausdrücklich vorsieht.

Der Gesetzgeber hat für die Verwaltungsdigitalisierung bereits eine passende Regelungstechnik entwickelt, die als Vorbild dienen kann. § 8 Abs. 8 Satz 3 OZG bindet den Dritten, an den Daten aus dem Nutzerkonto übermittelt werden, ausdrücklich an den Übermittlungszweck: Er darf die Daten, soweit gesetzlich nichts anderes bestimmt ist, nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt wurden. Eine solche ausdrückliche Zweckbindungsklausel empfiehlt sich auch für die spezialgesetzliche Absicherung der ZaPuK-Infrastruktur (vgl. 3.6.3 und 2.2).

3.2.4. Übertragung auf ZaPuK

Für ZaPuK ist die Zweckbindung – wie die Rechtmäßigkeit – auf zwei Ebenen zu beurteilen. Auf der Ebene der fachlichen Verarbeitung legen die kommunizierenden Stellen den Zweck der Inhaltsverarbeitung nach ihrem jeweiligen Fachrecht fest. Die domänenagnostische Infrastruktur (ADR-0001) trifft insoweit keine Aussage und kann den konkreten Zweck nicht vorwegnehmen. Aus der relativen Betrachtung des Personenbezugs folgt zugleich, dass sich die Frage der Zweckbindung hinsichtlich der Nachrichteninhalte für die reinen Backend-Betreiber nicht stellt, weil ihnen die Inhalte nur als Chiffrat vorliegen. Auf der Ebene des Infrastrukturbetriebs ist der Verarbeitungszweck demgegenüber eng auf die Ermöglichung der sicheren, vertraulichen und

nachweisbaren Kommunikation begrenzt. Jede darüberhinausgehende Verwendung der dabei anfallenden personenbezogenen Daten bedarf einer eigenständigen Rechtfertigung.

Praktisch wirkt die Zweckbindung damit vor allem auf der Metadatenebene, die trotz pseudonymer Adressierung für die Betreiber personenbezogen bleibt. Die Zielarchitektur setzt die Zweckbindung hier bereits an mehreren Stellen konsequent um. Die bereichsspezifische, pseudonyme Adressierung (ADR-1105) bindet die Erreichbarkeit an den jeweiligen Verwaltungsbereich und verhindert damit eine bereichsübergreifende Zusammenführung; sie ist der Sache nach eine Kontext- und Zweckbindung auf der Adressierungsebene. Die Betreibertrennung zwischen Bürger- und Organisationsdomäne und das in den Anschlussbedingungen vorgesehene Zusammenführungs- und Querzugriffsverbot (ADR-1145) verwirklichen die Zweckbindung als Instrument des Betreiberausschlusses (siehe 3.6.3): Metadaten, die zweckgebunden für die Übermittlung anfallen, dürfen nicht domänenübergreifend korreliert oder zu Profilbildungs- oder Überwachungszwecken weiterverwendet werden. Diese Vorgabe deckt sich mit der Wertung des § 3 Abs. 3 TDDDG.

Besondere Bedeutung hat die Zweckbindung für die bewusst erzeugten Nachweise. Die verpflichtende Bereitstellungsbestätigung (ADR-0018) erzeugt zusätzliche unverschlüsselte Metadaten (Zeitpunkt, Signatur, Nachrichtenreferenz), die allein dem Nachweiszweck der beweissicheren Bekanntgabe dienen. Sie sind auf diesen Zweck zu beschränken und dürfen nicht zu anderen Zwecken – etwa zur Verhaltens- oder Leistungskontrolle oder zur Auswertung von Kommunikationsmustern – weiterverwendet werden. Dass die demgegenüber freiwilligen Abruf- und Lesebestätigungen verschlüsselt übertragen werden und keine serverseitige Protokollierung auslösen (ADR-1118), entspricht dem Zweckbindungs- und Datenminimierungsgedanken. Auch die absendergesteuerten Zustelloptionen (ADR-1119) unterstützen die Zweckbindung, indem Nachweise und Metadaten nur dann erzeugt werden, wenn der konkrete Kommunikationszweck sie erfordert. Der Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111) vermeidet schließlich einen Datenbestand, dessen bloße Existenz zweckändernde Nutzungen nahelegen würde.

Eine zulässige Weiterverarbeitung zu einem geänderten Zweck kommt im Wesentlichen für die Aufbewahrung und Archivierung in Betracht, die im Machtbereich der jeweils verantwortlichen Stelle stattfindet und teilweise durch die Art. 5 Abs. 1 lit. b DSGVO privilegiert ist (ADR-1135, siehe 3.5.1). Für die im Betrieb anfallenden Protokoll- und Verkehrsdaten gilt die enge, im Abschnitt zu den Logdaten und – bei Einordnung als Telekommunikationsdienst – nach § 9 TDDDG konkretisierte Zweckbindung.

3.2.5. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Trennung zwischen der fachlich zweckgebundenen Inhaltsverarbeitung und der eng auf den Betriebszweck begrenzten Infrastrukturverarbeitung ist notwendig und beizubehalten. Die domänenagnostische Ausgestaltung (ADR-0001) ist folgerichtig: ZaPuK legt den fachlichen Zweck nicht fest, sondern muss die zweckgebundene Verarbeitung ermöglichen und dokumentierbar machen.

- Auf der weiterhin regulierten Metadatenebene ist die Zweckbindung das tragende Instrument des Betreiberausschlusses. Die bereichsspezifische pseudonyme Adressierung (ADR-1105), die Betreibertrennung und das Zusammenführungs- und Querzugriffsverbot (ADR-1145) sind zweckbindungsrechtlich geboten und im Einklang mit § 3 Abs. 3 TDDDG auszugestalten.

- Die bewusst erzeugten Nachweise sind strikt an ihren Zweck zu binden. Die Bereitstellungsbestätigung (ADR-0018) ist auf den Nachweis der Bekanntgabe zu beschränken; eine zweckfremde Auswertung – insbesondere zur Verhaltens- und Leistungskontrolle – ist auszuschließen. Die verschlüsselte, nicht serverseitig protokollierte Ausgestaltung der Abruf- und Lesebestätigungen (ADR-1118) ist beizubehalten.

- Eine Weiterverarbeitung zu anderen Zwecken bedarf entweder der Vereinbarkeit nach Art. 6 Abs. 4 DSGVO – wobei Verschlüsselung und Pseudonymisierung als geeignete Garantien zu Buche schlagen – oder einer gesonderten Rechtsgrundlage (§ 23 BDSG

bzw. Landesrecht; im JI-Bereich § 49 BDSG). Die Archivprivilegierung des Art. 5 Abs. 1 lit. b DSGVO greift nur unter den Garantien des Art. 89 Abs. 1 DSGVO (siehe 3.5.1).

- Die verbindliche Zweckbindung gegenüber den teilnehmenden Stellen und Betreibern ist über die Anschlussbedingungen (ADR-1145) zu transportieren. Dem Vorbild des § 8 Abs. 8 Satz 3 OZG folgend empfiehlt sich zusätzlich eine ausdrückliche spezialgesetzliche Zweckbindungs- und Verwendungsbeschränkung für die Infrastruktur- und Metadatenverarbeitung (siehe 3.6.3 und 2.2).

3.3. Datenminimierung

Kurzzusammenfassung. Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) verlangt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Verarbeitungszwecke notwendige Maß beschränkt sein müssen. Er ist kein absolutes Vermeidungsgebot im Sinne einer vollständigen Datensparsamkeit, sondern bemisst den zulässigen Umfang der Verarbeitung relativ zu dem – zuvor festgelegten – Zweck.

Für ZaPuK wirkt der Grundsatz auf drei Ebenen: der Menge der verarbeiteten Daten, der Identifizierbarkeit der betroffenen Personen und der Zugänglichkeit der Daten. Da der fachliche Zweck von der domänenagnostischen Infrastruktur (ADR-0001) nicht bestimmt wird, entfaltet die Datenminimierung ihre wesentliche Wirkung auf der Infrastrukturebene. Dort ist sie bereits weitgehend umgesetzt: durch die durchgängige Ende-zu-Ende-Verschlüsselung, die den Kreis der auf der Inhaltsebene überhaupt personenbezogen verarbeiteten Daten verengt, durch die Metadatenminimierung, durch die bereichsspezifische pseudonyme Adressierung, durch den Verzicht auf ein zentrales Adressregister für Privatpersonen sowie – als eigenständigen Beitrag – durch die selektive Offenlegung im fachlichen Identitätsnachweis und die bedarfsgesteuerte Erzeugung von Nachweisen. Die eng verwandten Aspekte der Erforderlichkeit sind bereits beim Grundsatz der Rechtmäßigkeit, die zeitliche Dimension (Speicherdauer, Löschung) beim Grundsatz der Speicherbegrenzung und die technische Umsetzung werden bei Art. 25 DSGVO behandelt (siehe 3.5).

3.3.1. Inhalt und Abgrenzung des Grundsatzes

Nach Art. 5 Abs. 1 lit. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Der Grundsatz betrifft damit den sachlichen Umfang der Verarbeitung: Verarbeitet werden dürfen nur solche Daten, die für den festgelegten Zweck geeignet und relevant sind, und auch diese nur in dem Umfang, der zur Zweckerreichung notwendig ist.

Datenminimierung ist dabei nicht mit einem absoluten Gebot der Datensparsamkeit gleichzusetzen. Die Verarbeitung muss nicht auf ein technisch mögliches Minimum reduziert werden; maßgeblich ist ein dem Zweck angemessenes Niveau. Ein eigenständiger Grundsatz der Datensparsamkeit, wonach jede Zielerreichung ohne personenbezogene Daten vorrangig wäre, ist in Art. 5 Abs. 1 lit. c DSGVO gerade nicht geregelt; der Verantwortliche darf den Verarbeitungszweck innerhalb der Grenzen zulässiger Verarbeitung festlegen und die Datenminimierung wird sodann an diesem Zweck gemessen.[269] Diese Relativität ist für ZaPuK bedeutsam: Die Infrastruktur kann den fachlichen Zweck der kommunizierenden Stellen nicht unterschreiten, wohl aber auf der eigenen Ebene sicherstellen, dass über das für den Betriebszweck Notwendige hinaus keine personenbezogenen Daten anfallen.

Der Grundsatz der Datenminimierung steht in engem Zusammenhang mit weiteren, an anderer Stelle behandelten Grundsätzen, ohne in ihnen aufzugehen. Die Frage, ob eine Verarbeitung für einen behördlichen Zweck erforderlich ist, und der hierfür maßgebliche, vom Europäischen Gerichtshof streng gehandhabte Verhältnismäßigkeitsmaßstab einschließlich des Verbots einer Datenerhebung „auf Vorrat" sind bereits beim Grundsatz der Rechtmäßigkeit dargestellt (siehe 3.1); die dortigen Ausführungen gelten hier entsprechend. Die zeitliche Dimension – wie lange Daten in identifizierbarer Form vorgehalten werden dürfen und wann sie zu löschen sind – ist Gegenstand des Grundsatzes der Speicherbegrenzung und wird dort behandelt (siehe 3.5). Die Umsetzung der Datenminimierung durch Technikgestaltung und datenschutzfreundliche Voreinstellungen schließlich konkretisiert Art. 25 DSGVO, dessen Absatz 2 die Menge der

[269] Vgl. *Kramer* in Auernhammer, 8. Auflage 2024, Art. 5 DSGVO Rn. 34.

erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit ausdrücklich erfasst; hierauf wird im gesonderten Abschnitt zu Art. 25 DSGVO eingegangen.

Jenseits dieser Überschneidungen verbleibt der Datenminimierung ein eigenständiger Gehalt, der für die Architektur von ZaPuK zentral ist. Er betrifft drei Bezugsgrößen: erstens die Menge und den Umfang der verarbeiteten Daten, zweitens die Identifizierbarkeit der betroffenen Personen – die durch Pseudonymisierung und Vermeidung stabiler, verkettbarer Kennungen zu verringern ist – und drittens die Zugänglichkeit der Daten, also die Begrenzung des Kreises der Stellen und Personen, denen die Daten offenstehen.

3.3.2. Bereichsspezifische Ausprägungen

Im Anwendungsbereich der JI-Richtlinie – für ZaPuK relevant, soweit über das Justiz-Backend zu den Zwecken des § 45 BDSG verarbeitet wird (siehe oben 1.2) – entspricht § 47 Nr. 3 BDSG dem Grundsatz der Datenminimierung: Personenbezogene Daten müssen dem Verarbeitungszweck entsprechen, für dessen Erreichen erforderlich sein und dürfen nicht außer Verhältnis zu ihm stehen. Verschärfend tritt § 71 BDSG hinzu, der – anders als die DSGVO – ausdrücklich von Datensparsamkeit spricht und die Verarbeitung und die Gestaltung der Datenverarbeitungssysteme an dem Ziel ausrichtet, so wenig personenbezogene Daten wie möglich zu verarbeiten. Nach § 71 Abs. 1 Satz 4 BDSG sind Daten zudem zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist. Diese Wertung der frühestmöglichen Pseudonymisierung lässt sich als Konkretisierung dessen heranziehen, was der Datenminimierungsgrundsatz auch außerhalb des JI-Rechts nahelegt, und stützt die pseudonyme Grundausrichtung der Adressierung.

3.3.3. Übertragung auf ZaPuK

Die Zielarchitektur verwirklicht den Grundsatz der Datenminimierung an mehreren Stellen und auf allen drei Bezugsgrößen. Sie stützt sich dabei auf dieselben Grundentscheidungen, die bereits die Anwendbarkeit des Datenschutzrechts prägen (siehe oben 1.3), verwendet sie hier aber unter dem Gesichtspunkt der Begrenzung des Datenanfalls.

a) Menge und Umfang

Die durchgängige Ende-zu-Ende-Verschlüsselung (ADR-0011, ADR-0012, ADR-1100) ist nicht nur eine Sicherheits-, sondern zugleich eine datenminimierende Maßnahme: Sie bewirkt, dass die Nachrichteninhalte für die reinen Transport- und Speicherakteure nicht personenbezogen sind und deren Verarbeitung auf der Inhaltsebene von vornherein außerhalb des Anwendungsbereichs bleibt (siehe 1.3). Auf der datenschutzrechtlich regulierten Metadatenebene setzt die Architektur das Grundziel, schützenswerte Metadaten möglichst gar nicht erst entstehen zu lassen (Metadatenreduktion). Der wirksamste Beitrag zur Datenminimierung besteht darin, dass personenbezogene Daten nicht anfallen. Hierzu zählen namentlich das für die Privatpersonen-Domäne vorgesehene Protokollierungsverbot für IP-Adressen und die domänengetrennte Betreiberstruktur. Auch der Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111) vermeidet einen umfangreichen personenbezogenen Datenbestand, der ohne zwingenden Betriebszweck vorgehalten würde.

b) Identifizierbarkeit

Die bereichsspezifische, pseudonyme Adressierung von Privatpersonen (ADR-1105) verringert die Identifizierbarkeit und die bereichsübergreifende Verkettbarkeit und setzt damit den Gedanken der frühestmöglichen Pseudonymisierung um. Besondere Bedeutung kommt dem fachlichen Identitätsnachweis zu: Durch die Wahl des Formats SD-JWT VC mit selektiver Offenlegung (ADR-1106, ADR-1107) werden dem Empfänger nur die für den jeweiligen Anwendungsfall zwingend benötigten Angaben (Claims) präsentiert, während nicht erforderliche Angaben zurückgehalten werden. Diese kontext- und bedarfsbezogene Offenlegung ist ein Musterbeispiel für Datenminimierung auf der Ebene der Identitätsdaten. Sie wird dadurch flankiert, dass die Nachweise im Regelfall keine Klarnamen oder Personalnummern enthalten, die organisationsinterne Mitarbeiteridentität die Organisation nicht verlässt und bei Privatpersonen stabile, empfängerübergreifende Identifier vermieden werden.

c) Zugänglichkeit

Die Begrenzung des Kreises der Zugriffsberechtigten – von Art. 25 Abs. 2 DSGVO ausdrücklich als Bezugsgröße der Datenminimierung genannt – wird über die bereichsspezifischen Postfächer, die auf die jeweilige Bearbeitergruppe beschränkte Sicht der Vorgangsräume und die nach Berechtigungen gefilterte aggregierte Postfachsicht (ADR-1102, ADR-1105) verwirklicht. Fachportale erhalten nur Zugriff auf die Kommunikation ihres Verwaltungsbereichs. Auf diese Weise wird nicht nur der Umfang der erhobenen, sondern auch der Umfang der offengelegten Daten auf das für den jeweiligen Zweck Notwendige beschränkt.

d) Bedarfsgesteuerte Nachweise

Der Grundsatz der Datenminimierung stützt schließlich die Entscheidung, Nachweise und die mit ihnen verbundenen zusätzlichen Metadaten nur dann zu erzeugen, wenn der konkrete Kommunikationszweck sie erfordert. Die absendergesteuerten Zustelloptionen (ADR-1119) erlauben es, den Umfang der erzeugten Nachweise am jeweiligen Anwendungsfall auszurichten, statt für jede Nachricht ein einheitliches Höchstmaß an Metadaten zu produzieren. Dass die freiwilligen Abruf- und Lesebestätigungen verschlüsselt übertragen werden und keine serverseitige Protokollierung auslösen (ADR-1118), entspricht ebenfalls dem Minimierungsgedanken. Ein Identitätsnachweis ist nicht bei jeder Kommunikation vorzusehen; für rein informelle Kommunikation oder Beratung kann auf ihn verzichtet werden (ADR-1106), was den Anfall personenbezogener Nachweisdaten weiter begrenzt. Zur zulässigen Vorhaltedauer der so anfallenden Daten und zu ihrer Löschung wird auf den Grundsatz der Speicherbegrenzung verwiesen.

3.3.4. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die datensparsamen Grundentscheidungen von ZaPuK sind auch am Maßstab der Datenminimierung nicht nur zulässig, sondern rechtlich geboten. Die durchgängige Ende-zu-Ende-Verschlüsselung, die Metadatenminimierung, die pseudonyme bereichsspezifische Adressierung und der Verzicht auf zentrale Datenbestände

begrenzen den Umfang der überhaupt personenbezogen verarbeiteten Daten und werden dadurch bestätigt.

- Die Datenminimierung ist relativ zum Zweck zu verstehen. Da die domänenagnostische Infrastruktur (ADR-0001) den fachlichen Zweck nicht festlegt, ist die Minimierung auf der Infrastrukturebene umzusetzen; die kommunizierende Stelle bleibt für die Begrenzung der von ihr im Klartext verarbeiteten Daten selbst verantwortlich.

- Die selektive Offenlegung im Identitätsnachweis (SD-JWT VC, ADR-1107) ist als eigenständiger Beitrag zur Datenminimierung beizubehalten und konsequent umzusetzen. Für jeden Anwendungsfall sollten die zwingend erforderlichen Pflichtangaben definiert und der Nachweisumfang hierauf beschränkt werden; die noch offene Festlegung des Nachweisschemas (ADR-1107) sollte an diesem Maßstab ausgerichtet werden. Klarnamen, Personalnummern und stabile, empfängerübergreifende Identifier sind zu vermeiden.

- Die Begrenzung der Zugänglichkeit ist als Teil der Datenminimierung fortzuführen: bereichsspezifische Postfächer, auf die Bearbeitergruppe beschränkter Vorgangszugriff und nach Berechtigungen gefilterte Sichten. Dies deckt sich mit den Anforderungen des Art. 25 Abs. 2 DSGVO und ist dort weiter zu behandeln.

- Nachweise und Metadaten sollten bedarfsgesteuert und nicht pauschal erzeugt werden. Die absendergesteuerten Zustelloptionen (ADR-1119) und die verschlüsselte, nicht serverseitig protokollierte Ausgestaltung der Abruf- und Lesebestätigungen (ADR-1118) sind aus Sicht der Datenminimierung beizubehalten.

- Die verbindliche Umsetzung gegenüber den teilnehmenden Stellen und Betreibern – insbesondere das Protokollierungsverbot für IP-Adressen, die Betreibertrennung und das Verbot der domänenübergreifenden Zusammenführung – ist über die Anschlussbedingungen (ADR-1145) sicherzustellen, ohne die eigenständige datenschutzrechtliche Verantwortung der jeweiligen Stelle zu verlagern (siehe 3.6.3).

3.4. Richtigkeit

Kurzzusammenfassung. Der Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) verlangt, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; für unrichtige Daten sind alle angemessenen Maßnahmen zu ihrer unverzüglichen Löschung oder Berichtigung zu treffen. Durchgesetzt wird er durch das Recht auf Berichtigung (Art. 16 DSGVO).

Der Grundsatz ist relativ zum Verarbeitungszweck zu verstehen und – für ZaPuK zentral – von den kryptografisch gesicherten Integritäts- und Authentizitätsmechanismen der Architektur zu trennen: Siegel, Signaturen und Prüfsummen (ADR-0017, ADR-0018) gewährleisten die Unveränderheit und die Herkunft eines Dokuments, nicht dessen sachliche Richtigkeit. Wie bei den übrigen Grundsätzen liegt die inhaltliche Richtigkeit der Nachrichten bei den kommunizierenden Stellen. Die domänenagnostische Infrastruktur (ADR-0001) trifft hierzu keine Aussage, und für die reinen Backend-Betreiber stellt sich die Frage der Richtigkeit im Sinne der DSGVO mangels Personenbezugs der verschlüsselten Inhalte nicht. Praktische Bedeutung entfaltet der Grundsatz auf der Infrastrukturebene vor allem für die Richtigkeit und Aktualität der Adress- und Zuordnungsdaten (ADR-1111), der Identitätsnachweise (ADR-1106, ADR-1107) und der Berechtigungen (ADR-1112); insoweit ist die Architektur bereits auf Richtigkeit und Aktualität angelegt.

3.4.1. Inhalt und Abgrenzung des Grundsatzes

Nach Art. 5 Abs. 1 lit. d DSGVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Verarbeitungszwecke unrichtige Daten unverzüglich gelöscht oder berichtigt werden. Der Grundsatz ist relativ zum Zweck anzuwenden, d.h. ob und wie aktuell ein Datum gehalten werden muss, bemisst sich am jeweiligen Verarbeitungszweck. Für den Bereich der Strafverfolgung und Gefahrenabwehr – bei ZaPuK relevant, soweit über das Justiz-Backend zu den Zwecken des § 45 BDSG verarbeitet wird – entspricht § 47 Nr. 4 BDSG dieser Vorgabe.

Richtigkeit meint die tatsächliche Korrektheit im Sinne einer zutreffenden Abbildung der Wirklichkeit, nicht die inhaltliche „Richtigkeit" einer Aussage oder Beurteilung. Für eine Kommunikationsinfrastruktur ist diese Unterscheidung von besonderer Bedeutung: Eine übermittelte Erklärung ist als Datum bereits dann richtig, wenn sie den tatsächlich abgegebenen Inhalt zutreffend wiedergibt; ob die in ihr enthaltene Aussage inhaltlich zutrifft oder bestritten wird, berührt die datenschutzrechtliche Richtigkeit nicht. Diese Wertung enthält § 58 Abs. 1 Satz 2 BDSG für den JI-Bereich ausdrücklich. Nachrichten sind zudem zeitpunktbezogene Kommunikationsakte und keine fortlaufend zu pflegenden Datensätze; sie werden nicht nachträglich „berichtigt", sondern durch neue Nachrichten korrigiert oder ergänzt.

Von der Richtigkeit strikt zu trennen ist der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO). Richtigkeit betrifft die inhaltliche Korrektheit, Integrität den Schutz vor unbefugter oder unbeabsichtigter Veränderung. Die kryptografischen Mechanismen von ZaPuK – das qualifizierte Siegel des Dokuments vor Versand (ADR-0017), der Ciphertext-Hash der Bereitstellungsbestätigung (ADR-0018) und die Signaturen der Nachweise – sichern damit Integrität und Authentizität, nicht die sachliche Richtigkeit. Sie belegen, dass ein Dokument unverändert von einer bestimmten Stelle stammt, treffen aber keine Aussage darüber, ob sein Inhalt zutrifft. Diese Mechanismen werden im Abschnitt zur Datensicherheit behandelt (siehe 3.6).

3.4.2. Übertragung auf ZaPuK

Auf der Ebene der fachlichen Inhalte liegt die Richtigkeit bei den kommunizierenden Stellen, die über den Klartext verfügen; die domänenagnostische Infrastruktur nimmt sie nicht vorweg. Aus der relativen Betrachtung des Personenbezugs folgt zugleich, dass sich die Frage der Richtigkeit hinsichtlich der Nachrichteninhalte für die reinen Backend-Betreiber nicht stellt, weil ihnen die Inhalte nur als Chiffrat vorliegen (siehe 1.3).

Praktisch wirkt der Grundsatz damit vor allem auf der Ebene der Adress-, Nachweis- und Berechtigungsdaten, die im Betrieb personenbezogen anfallen. Richtigkeitskritisch ist zunächst das Adressregister (ADR-1111) als die im Verbund verbindliche Quelle für die Zuordnung von Postfachadresse (MXID) und Organisation: Eine unrichtige Zuordnung führt unmittelbar zu

Fehlübermittlungen. Die Architektur setzt Richtigkeit hier durch die dezentrale Pflege der Einträge durch die jeweils zuständigen Betreiber, die kryptografische Signatur der Einträge und die verbindliche Prüfung von Adressen – insbesondere von in Anträgen angegebenen Rückantwortadressen – vor ihrer Verwendung um. Auch die Deaktivierung statt Löschung inaktiver Einträge, etwa bei einem Umzug über die well-known-Delegation, dient der Richtigkeit, weil sie die Zuordnung dauerhaft prüfbar hält. Für Privatpersonen wird die MXID deterministisch aus dem bereichsspezifischen Pseudonym abgeleitet (ADR-1105); dies sichert eine korrekte und stabile Zuordnung, ohne dass ein zentrales Register vorgehalten werden müsste.

Die Anforderung, Daten erforderlichenfalls auf dem neuesten Stand zu halten, betrifft ferner die Identitätsnachweise und die Berechtigungen. Die kurzlebigen, kontextbezogenen Nachweise (ADR-1106, ADR-1107) werden auf ihre Gültigkeit zum Versandzeitpunkt geprüft, und die Vorhaltung der historischen Schlüssel- und Statusverläufe erlaubt eine spätere, auf den maßgeblichen Zeitpunkt bezogene Prüfung. Ihre begrenzte Gültigkeitsdauer bewirkt zugleich, dass eine Sperrung oder eine Attributänderung zeitnah wirksam wird. Entsprechend setzt der Raum-Management-Service Änderungen der Postfachmitgliedschaften und Rechte aus dem Berechtigungsverzeichnis (ADR-1112) zeitnah um. Beides verwirklicht das Aktualitätsgebot des Art. 5 Abs. 1 lit. d DSGVO.

Das Recht auf Berichtigung (Art. 16 DSGVO; im JI-Bereich § 58, § 75 BDSG) richtet sich gegen die für die jeweilige Verarbeitung verantwortliche Stelle. Dass der Backend-Betreiber aufgrund der Ende-zu-Ende-Verschlüsselung Nachrichteninhalte nicht berichtigen kann, ist unschädlich: Die inhaltliche Richtigkeit obliegt den Endpunkten, und Nachrichten werden als Kommunikationsakte nicht nachträglich verändert, sondern durch neue Nachrichten korrigiert. Berichtigung und Aktualisierung greifen praktisch bei den Adress-, Nachweis- und Berechtigungsdaten und werden von den jeweils zuständigen Stellen – dem Register- bzw. Backendbetreiber, der Nachweisstelle und der Organisation über das Berechtigungsverzeichnis – umgesetzt.

3.4.3. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Trennung zwischen der fachlich getragenen Richtigkeit der Inhalte und der Richtigkeit der Infrastrukturdaten ist in der Zielarchitektur abgebildet. Ihr entspricht die domänenagnostische Ausgestaltung (ADR-0001): ZaPuK beurteilt die inhaltliche Richtigkeit nicht, muss die richtige Verarbeitung aber ermöglichen und die zuständige Stelle verantwortlich lassen.

- Richtigkeit ist von Integrität und Authentizität zu unterscheiden. Die kryptografischen Mechanismen (ADR-0017, ADR-0018) leisten Integritäts- und Herkunftssicherung; sie ersetzen keine Richtigkeitsprüfung und sind nicht als solche misszuverstehen. Die inhaltliche Richtigkeit bleibt Sache der absendenden Stelle.

- Das Adressregister ist die für die Richtigkeit kritische Komponente. Die vorgesehene verbindliche Adressprüfung vor Verwendung (insbesondere der Rückantwortadressen), die Signatur der Einträge, die dezentrale Pflege und die Deaktivierung statt Löschung entsprechen dem Grundsatz der Richtigkeit und erscheinen geboten. Da die Verlässlichkeit der Zuordnung von der Qualität des Registrierungs- und Pflegeprozesses abhängt, sollten diese Anforderungen über die Anschlussbedingungen (ADR-1145) verbindlich abgesichert werden.

- Die Aktualität ist über die Gültigkeits- und Sperrmechanismen der Identitätsnachweise (ADR-1106, ADR-1107) und die zeitnahe Umsetzung von Berechtigungsänderungen (ADR-1112) zu gewährleisten. Die Gültigkeitsdauer der Nachweise ist dabei so auszubalancieren, dass Sperrungen und Attributänderungen zeitnah wirken, ohne die Kommunikation zu behindern.

- Berichtigungsersuchen (Art. 16 DSGVO; im JI-Bereich § 58, § 75 BDSG) sind der jeweils verantwortlichen Stelle zuzuordnen. Nachrichteninhalte werden nicht nachträglich geändert, sondern durch neue Nachrichten korrigiert; die Berichtigung greift auf der Ebene der Adress-, Nachweis- und Berechtigungsdaten.

3.5. Speicherbegrenzung

Art. 5 DSGVO verpflichtet den Verantwortlichen, personenbezogene Daten nur so lange in identifizierbarer Form zu speichern, wie es für die Verarbeitungszwecke erforderlich ist (Art. 5 Abs. 1 lit. e DSGVO – Speicherbegrenzung), und sie auf das notwendige Maß zu beschränken (Art. 5 Abs. 1 lit. c DSGVO – Datenminimierung). Für ZaPuK folgt daraus, dass die Infrastruktur eine zeitlich begrenzte, zweckgebundene Vorhaltung ermöglichen und die Erfüllung von Lösch- und Aufbewahrungspflichten durch die jeweils verantwortlichen Stellen unterstützen muss, ohne diese – der domänenagnostischen Grundentscheidung (ADR-0001) folgend – selbst inhaltlich vorwegzunehmen.

3.5.1. Löschung und Archivierung

Kurzzusammenfassung:

Die über ZaPuK abgewickelte Kommunikation unterliegt zwei gegenläufigen Pflichtenrichtungen: Das Datenschutzrecht verlangt Datenminimierung und Löschung, sobald der Zweck erreicht ist; das Aktenführungs- und Archivrecht verlangt eine revisionssichere, teils langfristige Aufbewahrung aktenrelevanter Vorgänge und deren Anbietung an das zuständige Archiv.

Beide Richtungen lassen sich vereinbaren, wenn nach Aktenrelevanz und Datenart differenziert wird und die Prozesse in Lösch-, Aktenführungs- und Archivkonzepten verankert sind. Der datenschutzrechtliche Löschauftrag (Art. 5 Abs. 1 lit. e, Art. 17 DSGVO; § 35 BDSG) tritt zurück, soweit eine gesetzliche Aufbewahrungs- oder Archivierungspflicht besteht.

Zu trennen sind Inhaltsdaten (Maßstab: allgemeines Datenschutzrecht), unverschlüsselt anfallende Kommunikationsmetadaten und – soweit ein Postfach als Telekommunikationsdienst einzuordnen ist (siehe V) – Verkehrsdaten mit dem strengen Löschregime des § 9 TDDDG.

Für ZaPuK bedeutet dies: keine gesetzlich gebotene Dauervorhaltung im Postfach (siehe VII.1), Aufbewahrung und Archivierung im Machtbereich der jeweils verantwortlichen Stelle statt in einem zentralen Dienst (ADR-1135), konfigurierbare und nach Datenart differenzierte

Löschfristen sowie ein Nachweis der Löschung (Löschquittung, ADR-0018). Verbindlichkeit gegenüber den Teilnehmern ist über die Anschlussbedingungen herzustellen (ADR-1145).

a) Ausgangspunkt: das Spannungsverhältnis von Löschung und Aufbewahrung

Elektronische Verwaltungskommunikation steht in einem Spannungsverhältnis zweier gegenläufiger Pflichten. Einerseits sind personenbezogene Daten datenschutzrechtlich zu minimieren und zu löschen, sobald der Verarbeitungszweck erreicht ist und keine Aufbewahrungspflicht mehr besteht. Andererseits müssen aktenrelevante Unterlagen ordnungsgemäß und revisionssicher geführt, für die jeweils geltenden Fristen aufbewahrt und schließlich dem zuständigen Archiv angeboten werden. Diese beiden Anforderungen widersprechen einander nicht zwingend, sondern lassen sich rechtssicher zusammenführen, wenn nach Aktenrelevanz und Datenart unterschieden und die entsprechenden Abläufe in einem dokumentierten Lösch- und Aufbewahrungskonzept festgelegt werden.

b) Der datenschutzrechtliche Löschauftrag

Nach Art. 5 Abs. 1 lit. e DSGVO dürfen personenbezogene Daten nur so lange in einer die Identifizierung ermöglichenden Form gespeichert werden, wie es für die Verarbeitungszwecke erforderlich ist. Diese zeitliche Grenze wird durch die Löschpflicht des Art. 17 DSGVO konkretisiert und durchgesetzt: Sind die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig, sind sie grundsätzlich unverzüglich zu löschen (Art. 17 Abs. 1 lit. a DSGVO). Das nationale Recht ergänzt dies für die Fälle, in denen eine Löschung technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, um die Möglichkeit der Einschränkung der Verarbeitung an Stelle der Löschung (§ 35 Abs. 1 BDSG). Aus dem Erforderlichkeitsgrundsatz folgt zugleich, dass eine Speicherung „auf Vorrat" – allein für den Fall einer möglichen künftigen Nützlichkeit der Daten – nicht zulässig ist.[270] Die praktische Umsetzung der Speicherbegrenzung erfolgt über ein zu dokumentierendes Löschkonzept, das insbesondere die Zwecke, die

[270] *Eßer* in Auernhammer, 8. Auflage 2024, § 3 BDSG Rn. 28.

daraus abgeleiteten – gegebenenfalls nach Datenarten differenzierten – Speicher- und Aufbewahrungsfristen, die Löschverfahren und die Nachweisführung festlegt.[271]

c) Gegenläufige Aufbewahrungs- und Archivierungspflichten

Der Löschpflicht stehen gesetzliche Aufbewahrungs- und Archivierungspflichten gegenüber, die ihr vorgehen. Für die elektronische Aktenführung verlangt § 6a EGovG, dass die Grundsätze ordnungsgemäßer Aktenführung durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sichergestellt werden; hieraus folgen Anforderungen an Integrität, Nachvollziehbarkeit und Revisionssicherheit der geführten Akten. Für die langfristige Sicherung treten die Anbietungs- und Aussonderungspflichten des Archivrechts hinzu: Unterlagen, die zur Aufgabenerfüllung nicht mehr benötigt werden und deren weitere Aufbewahrung nicht besonders gestattet ist, sind dem Bundesarchiv anzubieten, spätestens 30 Jahre nach ihrer Entstehung (§ 5 Abs. 1 Bundesarchivgesetz (BArchG)); für geheimhaltungsbedürftige Unterlagen sowie für dem Steuergeheimnis unterliegende Unterlagen gilt § 6 BArchG. Bemerkenswert – und für die telekommunikationsrechtliche Einordnung von ZaPuK von Bedeutung – ist die Ausnahme des § 6 Abs. 2 Nr. 1 BArchG: Unterlagen, deren Offenbarung gegen das Brief-, Post- oder Fernmeldegeheimnis verstößt, sind von der Anbietungspflicht ausgenommen.

Systematisch löst die DSGVO das Verhältnis zugunsten der Aufbewahrung: Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke gilt nicht als mit dem ursprünglichen Zweck unvereinbar (Art. 5 Abs. 1 lit. b DSGVO), und eine längere Speicherung ist für solche Archivzwecke ausdrücklich zulässig, sofern die Garantien des Art. 89 Abs. 1 DSGVO – insbesondere technische und organisatorische Maßnahmen zur Wahrung der Datenminimierung – eingehalten werden (Art. 5 Abs. 1 lit. e DSGVO). Die Löschpflicht des Art. 17 DSGVO gilt dementsprechend nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist (Art. 17 Abs. 3 lit. b DSGVO) oder Archivzwecken dient (Art. 17 Abs. 3 lit. d DSGVO); ergänzend stellt § 35 Abs. 3 BDSG klar, dass Aufbewahrungsfristen einer Löschung entgegenstehen. Die datenschutzrechtliche Löschung und die archivrechtliche Sicherung greifen zudem ineinander: Nach Übernahme

[271] Kramer, in: Auernhammer, 8. Auflage 2024, Art. 5 DSGVO, Rn. 54a.

durch das Archiv und nach Ablauf der Aufbewahrungsfrist sind bei der abgebenden Stelle verbliebene Kopien nach dem Stand der Technik zu löschen, und über die Löschung ist ein Nachweis zu fertigen (§ 5 Abs. 3 BArchG).

Für ZaPuK löst sich das beschriebene Spannungsverhältnis durch die schon in den vorangegangenen Abschnitten angelegte Rollenteilung: Die revisionssichere Langzeitsicherung aktenrelevanter Vorgänge liegt in der behördlichen Sphäre – der elektronischen Aktenführung und dem Archivrecht der jeweils zuständigen Stelle – und nicht im Bürger- oder Organisationspostfach der Infrastruktur. Das Postfach ist Kommunikations- und Zugangskanal, nicht Archivsystem (dazu VII.1).

d) Inhaltsdaten, Metadaten und telekommunikationsrechtliches Löschregime

Die Lösch- und Aufbewahrungsfrage ist nach Datenart zu differenzieren. Für die Inhaltsdaten gilt das allgemeine Datenschutzrecht (Art. 5, Art. 17 DSGVO). Für die im Postfach-Backend zwangsläufig unverschlüsselt anfallenden Kommunikationsmetadaten gilt es ebenfalls, weil diese – anders als die Inhalte – für die Betreiber trotz pseudonymer Adressierung personenbezogen bleiben (siehe 1.3). Soweit ein Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu V), tritt für Verkehrsdaten das strenge Regime des § 9 TDDDG hinzu: Verkehrsdaten dürfen nur zu den dort genannten Zwecken verarbeitet werden und sind im Übrigen nach Beendigung der Verbindung unverzüglich zu löschen (§ 9 Abs. 1 Satz 2 und 3 TDDDG). Inhalts-, Metadaten- und Verkehrsdaten sind daher mit jeweils eigenen, gesetzeskonformen Löschregimen zu versehen und nicht einheitlich zu behandeln.

Aus der relativen Betrachtung des Personenbezugs (1.3) ergibt sich zugleich eine Präzisierung, wer den Löschauftrag hinsichtlich der Inhalte schuldet. Da die Inhaltsdaten für die reinen Backend-Betreiber mangels Schlüsselzugriff nicht personenbezogen sind, trifft die inhaltsbezogene Speicherbegrenzung und Löschung primär die Stellen mit Klartextzugriff – die Endgeräte, die versendenden Stellen und etwaige serverseitige Entschlüsselungsendpunkte. Das Backend kann und muss die Speicherbegrenzung auf der Ebene der bei ihm anfallenden Daten umsetzen, indem es das gespeicherte Chiffrat sowie die personenbezogenen Metadaten nach Maßgabe konfigurierter Fristen tatsächlich löscht; die Löschung des Chiffrats bewirkt – unabhängig

vom Schlüssel – eine wirksame Beseitigung der Inhaltsverfügbarkeit. Eine inhaltsbezogene, an den Nachrichtentext anknüpfende Löschentscheidung kann das Backend hingegen aufgrund der Ende-zu-Ende-Verschlüsselung nicht treffen; sie bleibt den Endpunkten vorbehalten.

e) Übertragung auf ZaPuK

Die Zielarchitektur bildet das skizzierte Regime bereits weitgehend zutreffend ab. ZaPuK stellt keinen zentralen Aufbewahrungsdienst bereit; die Übernahme in Facharchive und E-Akte-Systeme erfolgt im Machtbereich der jeweiligen Datenbesitzer über die Endgeräte oder über einen als E2EE-Teilnehmer konfigurierten technischen Nutzer, ergänzt um ein standardisiertes Exportpaket mit den zugehörigen Nachweisartefakten (ADR-1135). Diese Verortung entspricht der gesetzlichen Zuweisung der Langzeitsicherung an die behördliche Sphäre (§ 6a EGovG, §§ 5, 6 BArchG) und vermeidet zugleich eine datenschutzrechtlich problematische zentrale Datenkonzentration. Für die Vorhaltung im Postfach selbst besteht keine gesetzliche Dauervorhaltepflicht; erforderlich und geboten ist lediglich, dass abgerufene Dokumente durch die Nutzenden gespeichert bzw. exportiert werden können (siehe VII.1).

Ergänzungsbedarf besteht bei der verbindlichen Ausgestaltung der Lösch- und Vorhaltefristen. Der Grundsatz der Speicherbegrenzung verlangt, dass die im Backend gespeicherten Chiffrate und Metadaten nicht unbefristet vorgehalten werden, sondern nach definierten, begründeten und nach Datenart differenzierten Fristen gelöscht werden. Die hierfür vorgesehene Umsetzung über konfigurierbare Löschfristen (in Ausarbeitung befindliche Folge-Entscheidung; technisch etwa über Matrix Retention Policies) ist datenschutzrechtlich folgerichtig, muss aber gewährleisten, dass Verkehrsdaten dem engeren Regime des § 9 TDDDG unterworfen werden und getrennt von den Inhaltsdaten behandelt werden. Die Löschquittung nach ADR-0018 erfüllt dabei zugleich die archiv- und nachweisrechtliche Funktion eines dokumentierten Löschnachweises und harmoniert mit der Nachweispflicht des § 5 Abs. 3 BArchG.

Weil ZaPuK als domänenagnostische Infrastruktur (ADR-0001) die fachspezifischen Aufbewahrungs- und Löschfristen nicht selbst bestimmen kann – diese richten sich nach dem jeweils anwendbaren Fach-, Aktenführungs- und Archivrecht der verantwortlichen Stelle –, muss die Architektur die Konfiguration und den Nachweis solcher Fristen ermöglichen, ohne sie zu

präjudizieren. Die verbindliche Absicherung gegenüber den teilnehmenden Stellen und Betreibern – insbesondere die Pflicht, verfahrensrelevante Inhalte erst nach deren Archivierung zu löschen und Aufbewahrungsfristen einzuhalten – ist über die Anschlussbedingungen zu transportieren; die konkrete Ausgestaltung der Aufbewahrungsfristen und Löschprozesse ist dort bislang als offener Punkt vermerkt (ADR-1145) und sollte im weiteren Verlauf präzisiert werden.

f) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Grundentscheidung, keinen zentralen Aufbewahrungsdienst vorzusehen und die Veraktung/Archivierung im Machtbereich der jeweils verantwortlichen Stelle zu belassen (ADR-1135), ist aus Sicht der Speicherbegrenzung folgerichtig. Sie weist die langfristige Sicherung der gesetzlich zuständigen Sphäre (§ 6a EGovG, §§ 5, 6 BArchG) zu und vermeidet eine zentrale Metadaten- und Inhaltskonzentration.

- Eine gesetzliche Pflicht zur dauerhaften Vorhaltung abgerufener Nachrichten im Postfach besteht nicht. Architektonisch genügend und geboten ist eine niederschwellige Export- bzw. Speicherfunktion für die Nutzenden (siehe VII.1). Die Vorhaltedauer im Postfach ist als begründete, am Maßstab von Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 lit. c und e DSGVO) ausgerichtete Gestaltungsentscheidung festzulegen.

- Die im Backend gespeicherten Chiffrate und Metadaten sind nach definierten, differenzierten Löschfristen tatsächlich zu löschen. Das vorgesehene, konfigurierbare Löschfristenregime sollte Inhaltsdaten, Kommunikationsmetadaten und – bei Einordnung als Telekommunikationsdienst – Verkehrsdaten (§ 9 TDDDG) mit jeweils eigenen Fristen versehen. Die Löschung ist nachzuweisen; die Löschquittung (ADR-0018) ist hierfür geeignet.

- Da die inhaltsbezogene Löschung wegen der Ende-zu-Ende-Verschlüsselung nicht serverseitig anhand des Nachrichtentexts erfolgen kann, ist die Verantwortung für die zweckbezogene Löschung der Inhalte den Klartext-Endpunkten (Endgeräte,

versendende Stellen, serverseitige Entschlüsselungsendpunkte) zuzuordnen. Das Backend setzt die Speicherbegrenzung durch fristgerechte Löschung des gespeicherten Chiffrats und der Metadaten um.

- Fachspezifische Aufbewahrungs- und Löschfristen kann die domänenagnostische Infrastruktur (ADR-0001) nicht selbst festlegen. Sie sind konfigurierbar zu halten und über die Anschlussbedingungen (ADR-1145) verbindlich zu machen; die dort noch offene Ausgestaltung der Aufbewahrungs- und Löschprozesse sollte konkretisiert werden, einschließlich der Pflicht, verfahrensrelevante Inhalte erst nach ihrer Archivierung zu löschen.

Von der Vorhaltung der Nachrichten- und Metadatenbestände zu unterscheiden ist die Behandlung der beim Betrieb anfallenden Protokoll- und Logdaten, die einem eigenen Zweck- und Fristenregime unterliegen; sie wird im folgenden Abschnitt gesondert behandelt.

3.5.2. Logdaten

Kurzzusammenfassung.

Logdaten – d.h. die beim Betrieb automatisch erzeugten Protokolle über System- und Zugriffsvorgänge – sind regelmäßig personenbezogen (IP-Adressen, Gerätekennungen, MXIDs, Zeitstempel) und unterliegen daher den datenschutzrechtlichen Verarbeitungsgrundsätzen; maßgeblich ist auch hier der relative Personenbezug (siehe 1.3).

Logdaten stehen in einem Spannungsverhältnis: Als Datensicherheits- und Rechenschaftsmaßnahme sind sie nach Art. 32 und Art. 5 Abs. 2 DSGVO geboten und im IT-Grundschutz Standard; zugleich muss ihre Generierung und Aufbewahrung der Datenminimierung, Zweckbindung und Speicherbegrenzung (Art. 5 Abs. 1 lit. b, c, e DSGVO) genügen.

Eine allgemeine gesetzliche Protokollierungspflicht besteht im DSGVO-Bereich nicht; im JI-Bereich (Justiz-Backend, soweit zu JI-Zwecken verarbeitet wird) ordnet § 76 BDSG eine Protokollierung mit strenger Zweckbindung und fester Löschfrist an. Diese Wertung – enge

Zweckbindung plus feste Löschung – kehrt in zahlreichen bereichsspezifischen Protokollierungsnormen wieder und dient als Orientierungsmaßstab auch außerhalb des JI-Rechts.

Für ZaPuK ergibt sich ein Gleichlauf mit den Grundentscheidungen: möglichst kein Anfall von Logdaten (Metadatenminimierung, Protokollierungsverbot für IP-Adressen, Betreibertrennung), für notwendige Protokolle eine ausdrückliche Zweckbindung, definierte kurze Löschfristen und ein Verbot der zweck- und domänenübergreifenden Auswertung. Zwei Sonderfälle bewusst erzeugter Protokolle – die verpflichtende Bereitstellungsbestätigung (ADR-0018) und die revisionssichere Protokollierung administrativer Änderungen (ADR-1102) – sind an ihren jeweiligen Zweck zu binden.

a) Ausgangspunkt: Begriff und Personenbezug von Logdaten

Als Logdaten werden die beim Betrieb eines IT-Systems automatisch geführten Protokolle über Aktionen und Prozesse bezeichnet – etwa Systemanmeldungen, Netzwerknutzung, Zugriffe auf Datensätze und administrative Vorgänge. Solche Protokolle enthalten regelmäßig personenbezogene Daten in Form von IP-Adressen, Gerätekennungen, Kennungen der handelnden Personen oder Zeitstempeln.[272] Ob ein bestimmter Logbestand für einen bestimmten Akteur personenbezogen ist, beurteilt sich nach dem relativen Maßstab (siehe 1.3); für die Betreiber der ZaPuK-Backends sind die im Klartext anfallenden Betriebs- und Zugriffsprotokolle typischerweise personenbezogen, weil sie den zugehörigen Kommunikationsvorgängen und – über die pseudonymen MXIDs mittelbar – den Beteiligten zugeordnet werden können. Logdaten sind damit auf derselben regulatorischen Ebene behandelten Kommunikationsmetadaten (siehe 1.1.3) und teilen deren Schutzbedürftigkeit. Von den Nachrichteninhalten unterscheiden sich Logdaten grundlegend: Während die Inhalte durch die Ende-zu-Ende-Verschlüsselung für die reinen Transport- und Speicherakteure anonym bleiben, fallen Logdaten auf der Betriebsebene an und sind von der Wirkung der E2EE nicht erfasst. Der besondere Schutzbedarf von Kommunikationsmetadaten – bis hin zu Risiken für die nationale Sicherheit bei massenhafter Korrelation – trifft Logdaten in gleicher Weise.

[272] Jandt, in: Hornung/Schallbruch IT-Sicherheitsrecht, § 17, Rn. 49.

b) Protokollierung im Spannungsverhältnis zwischen Datensicherheit/Nachweisbarkeit und Datenminimierung

Die Protokollierung ist zunächst eine Datensicherheitsmaßnahme. Sie macht nachvollziehbar, wer wann welche personenbezogenen Daten eingesehen oder verändert hat, und dient damit der Gewährleistung von Integrität und Vertraulichkeit (Art. 32 DSGVO) sowie der Erfüllung der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO). Im IT-Grundschutz ist die Protokollierung eine Standardmaßnahme.[273] Für ZaPuK ergibt sich der Sicherheits- und Nachweisbedarf zusätzlich aus dem IT-sicherheitsrechtlichen Rahmen (dazu IV), insbesondere der IT-Sicherheitsverordnung Portalverbund (ITSiV-PV), die für die IT-Komponenten des Portalverbunds Maßnahmen nach dem Stand der Technik und ein ISMS verlangt. Da Protokollierung jedoch zugleich personenbezogene Daten erzeugt, stehen dem mit ihr verfolgten Sicherheits- und Nachweisinteresse stehen die datenschutzrechtlichen Leitgrundsätze gegenüber. Soweit Logdaten nur den laufenden Nutzungsvorgang ermöglichen, entfällt ihr Zweck mit dessen Ende, sodass sie zu löschen wären; ihre über diesen Zeitpunkt hinausgehende Aufbewahrung zur nachträglichen Aufklärung von Unregelmäßigkeiten steht dagegen im Spannungsverhältnis zu Datenminimierung, Zweckbindung und Speicherbegrenzung.[274] Werden Logdaten von vornherein allein zur späteren Aufklärung erhoben, nähert sich dies einer Vorratsdatenspeicherung, die dem Grundsatz der Zweckbindung widerspricht.[275] Die Auflösung dieses Spannungsverhältnisses erfolgt nicht durch Verzicht auf Protokollierung, sondern durch deren risiko- und zweckangemessene Begrenzung: Erhebung nur des Erforderlichen, strikte Zweckbindung und eine begründete, möglichst kurze Speicherfrist.

c) Keine allgemeine Protokollierungspflicht – das JI-Regime als Orientierung

Eine ausdrückliche, allgemeine Pflicht zur Protokollierung enthält die DSGVO nicht; die Protokollierung ist dort Bestandteil der risikoabhängigen Pflichten aus Art. 32 und Art. 25 DSGVO und damit Ergebnis einer Abwägung, nicht einer starren Vorgabe. Anders liegt es im

[273] Kramer/Meints, in: Auernhammer, 8. Aufl. 2024, § 76 BDSG, Rn. 5; Jandt, in: Hornung/Schallbruch IT-SicherheitsR-HdB, § 17, Rn. 49.
[274] Jandt, in: Hornung/Schallbruch, IT-SicherheitsR-HdB, § 17, Rn. 49 f.
[275] Jandt, in: Hornung/Schallbruch, IT-SicherheitsR-HdB, § 17, Rn. 50.

Anwendungsbereich der JI-Richtlinie: § 76 BDSG verpflichtet Verantwortliche und Auftragsverarbeiter, in automatisierten Verarbeitungssystemen mindestens Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung zu protokollieren (§ 76 Abs. 1 BDSG). Für ZaPuK ist dieses Regime insoweit unmittelbar von Bedeutung, als das Justiz-Backend Verarbeitungen zu JI-Zwecken ermöglichen kann (siehe 1.2); maßgeblich ist auch hier nicht die Organisation, sondern der Verarbeitungszweck. Aufschlussreich sind vor allem die von § 76 BDSG angeordneten Grenzen. Absatz 3 enthält einen strengen Zweckbindungsgrundsatz: Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Verarbeitung, für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der Daten sowie für Strafverfahren verwendet werden; jede spätere Einführung eines weiteren Nutzungszwecks – insbesondere eine Verwendung zur Verhaltens- und Leistungskontrolle von Beschäftigten – ist untersagt (§ 76 Abs. 3 BDSG).[276] Absatz 4 ergänzt eine feste Löschfrist: Protokolldaten sind am Ende des auf ihre Generierung folgenden Jahres zu löschen (§ 76 Abs. 4 BDSG). Diese Kombination aus enger Zweckbindung und fixer Löschfrist ist kein Spezifikum des JI-Rechts, sondern eine wiederkehrende Regelungstechnik des Gesetzgebers für Protokolldaten. Sie findet sich – mit auf Datenschutzkontrolle, Datensicherung und ordnungsgemäßen Betrieb beschränkter Zweckbindung und regelmäßig ein- oder zweijähriger Löschfrist – etwa in § 9 Antiterrordateigesetz, § 11 Visa-Warndateigesetz und § 7 UBRegG. Für den nicht dem JI-Recht unterfallenden Teil von ZaPuK lassen sich diese Wertungen als Konkretisierung dessen heranziehen, was Datenminimierung, Zweckbindung und Speicherbegrenzung für Logdaten verlangen, auch wenn dort keine gesetzliche Protokollierungspflicht besteht.

d) Abgrenzung zu den Verkehrsdaten des TK-Rechts

Von den datenschutzrechtlich zu beurteilenden Betriebs- und Zugriffsprotokollen zu trennen sind die Verkehrsdaten, die entstehen, soweit ein Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu V). Für sie gilt das engere Regime des § 9 TDDDG mit unverzüglicher Löschung nach Beendigung der Verbindung, sofern kein gesetzlich zugelassener Zweck vorliegt (siehe oben 3.5.1). Eine eigenständige, aber ebenfalls eng zweckgebundene

[276] Vgl. Kramer/Meints, in: Auernhammer, 8. Aufl. 2024, § 76 BDSG, Rn. 17.

Verarbeitung erlaubt § 12 TDDDG für das Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern; auch dort sind die Daten unverzüglich zu löschen, sobald sie für die Störungsbeseitigung nicht mehr erforderlich sind, und eine Verarbeitung zu anderen Zwecken ist unzulässig (§ 12 Abs. 1 und 2 TDDDG).

Für die Architektur folgt daraus, dass Störungs- und Sicherheitsprotokolle, die zugleich Verkehrsdaten enthalten, nicht dem allgemeinen Logdaten-Regime, sondern den strengeren Vorgaben des TDDDG zu unterwerfen sind; Verkehrsdaten, allgemeine Logdaten und Inhaltsdaten sind daher mit jeweils eigenen Löschregimen zu versehen.

e) Übertragung auf ZaPuK

Die Zielarchitektur behandelt das Logdaten- und Metadatenaufkommen bereits als eigenständiges Schutzproblem und verfolgt als Grundziel, dass schützenswerte Metadaten möglichst gar nicht erst anfallen (Metadatenreduktion). Diese Linie ist datenschutzrechtlich folgerichtig: Der wirksamste Beitrag zur Datenminimierung besteht darin, protokollierbare personenbezogene Daten zu vermeiden. Konkret schlägt sich dies in der pseudonymen, bereichsspezifischen Adressierung, in der Betreibertrennung zwischen Bürger- und Organisationsdomäne und in dem für die Privatpersonen-Domäne vorgesehenen Verbot der Protokollierung von IP-Adressen nieder (vgl. ADR-1105). Diese Maßnahmen wirken zugleich als Absicherung des Betreiberausschlusses (siehe 3.6.3), weil nicht erhobene oder domänengetrennt gehaltene Logdaten nicht domänenübergreifend korreliert werden können.

Wo Logdaten für Sicherheit und Betrieb dennoch erforderlich sind, greifen die aus Art. 5, 25 und 32 DSGVO abgeleiteten und durch die JI-rechtliche Wertung konkretisierten Anforderungen: eine ausdrückliche Festlegung der zulässigen Zwecke (IT-Sicherheit, Störungsbeseitigung, Nachweis der Rechtmäßigkeit), ein Verbot der zweckwidrigen Weiterverwendung – insbesondere zur Beschäftigtenkontrolle – sowie definierte, möglichst kurze Löschfristen. Die verbindliche Ausgestaltung gegenüber den Betreibern erfolgt über die Anschlussbedingungen, die bereits eine nur zweckgebundene Auswertung betriebsbedingt anfallender Metadaten und Verbindungsdaten sowie ein Zusammenführungs- und Querzugriffsverbot zwischen den Domänen vorsehen (ADR-1145). Diese Anschlussbedingung sollte um ausdrückliche Vorgaben zu

Zweckbindung und Löschfristen der Logdaten ergänzt werden; deren Konkretisierung ist dort bislang als offener Punkt vermerkt.

Zwei Konstellationen betreffen bewusst erzeugte Protokolle und sind gesondert zu würdigen. Erstens erzeugt die verpflichtende Bereitstellungsbestätigung zusätzliche, unverschlüsselte Metadaten im Postfach-Backend (Zeitpunkt, Signatur, Nachrichtenreferenz), die dem Nachweiszweck der beweissicheren Übermittlung dienen (ADR-0018). Hierbei handelt es sich um eine zweckgebundene, für die rechtssichere Bekanntgabe erforderliche Protokollierung; sie ist datenschutzrechtlich als geeignete und für ihren Zweck erforderliche Maßnahme einzuordnen, muss aber auf diesen Zweck beschränkt bleiben und in ihrer Aufbewahrung an den Aufbewahrungs- und Nachweisbedarf des jeweiligen Vorgangs gekoppelt werden. Dass die demgegenüber freiwilligen Abruf- und Lesebestätigungen verschlüsselt übertragen werden und gerade keine serverseitige Protokollierung durch den Application Service auslösen (ADR-1118), ist aus Sicht der Datenminimierung und des Metadatenschutzes folgerichtig. Zweitens ist die revisionssichere Protokollierung administrativer Änderungen an Vorgangsräumen, Gruppen und Vertretungsregelungen (ADR-1102) sowie der Aktionen serverseitiger Entschlüsselungsendpunkte (ADR-1130) eine berechtigte, der Auditierung und Rechenschaft dienende Protokollierung im Machtbereich der jeweiligen Organisation; sie ist an diesen Zweck zu binden und mit einer definierten Aufbewahrungsfrist zu versehen.

f) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Das Grundziel der Metadatenreduktion ist auch für Logdaten der wirksamste Beitrag zur Datenminimierung. Das für die Privatpersonen-Domäne vorgesehene Protokollierungsverbot für IP-Adressen und die domänengetrennte Betreiberstruktur (ADR-1105) sind datenschutzrechtlich geboten und sichern zugleich den Betreiberausschluss (siehe 3.6.3).
- Für unvermeidbare Betriebs- und Zugriffsprotokolle sollten in den Anschlussbedingungen (ADR-1145) ausdrücklich die zulässigen Zwecke festgelegt, eine zweckwidrige

Weiterverwendung – insbesondere zur Verhaltens- und Leistungskontrolle von Beschäftigten – ausgeschlossen und definierte, möglichst kurze Löschfristen bestimmt werden. Die JI-rechtliche Wertung des § 76 BDSG sowie die Regelungstechnik vergleichbarer Protokollierungsnormen (enge Zweckbindung, feste Löschfrist) dienen dabei als Orientierungsmaßstab.

- Soweit ZaPuK-Verarbeitungen dem JI-Recht unterfallen (Justiz-Backend, zweckabhängig), ist die Protokollierung nach § 76 BDSG einschließlich der strengen Zweckbindung (Abs. 3) und der Löschfrist zum Ende des Folgejahres (Abs. 4) einzuhalten. Die Architektur muss eine solche zweck- und fristgebundene Protokollierung ermöglichen, ohne sie auf die nicht dem JI-Recht unterfallenden Verarbeitungen zu übertragen.

- Verkehrsdaten sind – bei Einordnung als Telekommunikationsdienst (siehe D.V.) – von den allgemeinen Logdaten zu trennen und dem engeren Regime der §§ 9, 12 TDDDG mit unverzüglicher, zweckgebundener Löschung zu unterwerfen. Verkehrsdaten, allgemeine Logdaten und Inhaltsdaten sind mit jeweils eigenen Löschregimen zu versehen (siehe 3.5.1).

- Bewusst erzeugte, als Nachweis dienende Protokolle sind an ihren Zweck zu binden. Die verpflichtende Bereitstellungsbestätigung (ADR-0018) ist auf den Beweiszweck zu beschränken und an den vorgangsbezogenen Nachweisbedarf zu koppeln; die revisionssichere Protokollierung administrativer Änderungen und der Aktionen serverseitiger Entschlüsselungsendpunkte (ADR-1102, ADR-1130) ist zweckgebunden und mit definierter Aufbewahrungsfrist auszugestalten. Die verschlüsselte, nicht serverseitig protokollierte Ausgestaltung der Abruf- und Lesebestätigungen (ADR-1118) ist aus Sicht des Metadatenschutzes beizubehalten.

3.6. Integrität und Vertraulichkeit (Datensicherheit)

Kurzzusammenfassung. Der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) verlangt, dass personenbezogene Daten in einer Weise verarbeitet werden, die durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit

gewährleistet, insbesondere Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Er wird durch Art. 32 DSGVO (Sicherheit der Verarbeitung) konkretisiert, der ein am Stand der Technik und am Risiko ausgerichtetes Schutzniveau fordert und dabei Pseudonymisierung und Verschlüsselung ausdrücklich als geeignete Maßnahmen nennt. Für ZaPuK ist dieser Grundsatz von zentraler Bedeutung, weil über die Infrastruktur massenhaft und potenziell hochsensible Kommunikation abgewickelt wird und die architekturprägenden Grundentscheidungen – durchgängige Ende-zu-Ende-Verschlüsselung, kryptografische Nachweise und Metadatenminimierung – unmittelbar diesem Grundsatz dienen.

Innerhalb dieses Abschnitts werden die datensicherheitsrechtlichen Kernfragen der Architektur behandelt: die Sicherung der Integrität (systemseitig oder kryptografisch), die Vertraulichkeit der Nachrichteninhalte durch Verschlüsselung – einschließlich ihrer rechtlichen Verbindlichkeit, ihrer Reichweite und Terminierung, der Zulässigkeit serverseitiger Verarbeitung, der Vereinbarkeit mit Archivierung und Stellvertretung sowie des Schlüsselmanagements und seiner Auswirkung auf den wirksamen Zugang – und schließlich die Vertraulichkeit der Kommunikationsbeziehungen auf der Metadatenebene (Betreiberausschluss).

Zwei Abgrenzungen sind vorab zu treffen. Der hier maßgebliche Maßstab des Standes der Technik kehrt im IT-Sicherheitsrecht wieder (etwa § 30 BSI-Gesetz (BSIG), § 165 Telekommunikationsgesetz (TKG), ITSiV-PV); er wird an dieser Stelle als Kern des Art. 32 DSGVO entfaltet, während seine bereichsspezifische Ausprägung im IT-sicherheitsrechtlichen Teil vertieft wird (siehe IV.). Ebenso ist die technische Umsetzung der Sicherheitsanforderungen durch Datenschutz durch Technikgestaltung Gegenstand des Art. 25 DSGVO und wird dort behandelt; der Nachweis der Wirksamkeit der Maßnahmen (Art. 32 Abs. 1 lit. d, Art. 5 Abs. 2 DSGVO) ist Teil der Rechenschaftspflicht und wird im entsprechenden Abschnitt aufgegriffen.

3.6.1. Integrität: systemseitig sicherstellen oder kryptografisch?

Die Integrität (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b DSGVO) betrifft den Schutz der Daten vor unbefugter oder unbeabsichtigter Veränderung. Zu ihrer Sicherung kommen zwei Wege in Betracht: eine rein systemseitig-organisatorische Absicherung (Zugriffskontrollen, Rollenmodell,

Protokollierung, Vier-Augen-Prinzip), die eine Veränderung vor allem nachträglich dokumentiert, und eine kryptografische Sicherung (Signatur, Siegel, Prüfsumme, versiegelter Zeitstempel), die eine Veränderung verhindert oder zumindest zuverlässig erkennbar macht. Angesichts des hohen Schutzbedarfs und der massenhaften Übermittlung potenziell hochsensibler Nachrichten über ZaPuK ist eine rein organisatorische Absicherung nicht risikoangemessen; die kryptografische Integritätssicherung ist geboten und entspricht insoweit auch dem Stand der Technik. Wo eIDAS-Vertrauensdienste oder Formerfordernisse eingreifen, sind kryptografische Mechanismen ohnehin zwingend. Die architekturprägenden Grundentscheidungen von ZaPuK – kryptografische Integrität im Kommunikationskanal, qualifiziertes Siegel des Dokumenteninhalts vor Versand und signierte, an das Chiffrat gebundene Übermittlungsnachweise – verwirklichen dies.

a) Inhalt und Maßstab des Integritätsschutzes

Art. 5 Abs. 1 lit. f DSGVO fasst Integrität und Vertraulichkeit zu einem Grundsatz zusammen. Die Integrität zielt dabei auf den Schutz vor Veränderung, während die Vertraulichkeit den Schutz vor unbefugter Kenntnisnahme betrifft. Konkretisiert wird der Grundsatz durch Art. 32 DSGVO, der die Fähigkeit verlangt, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b DSGVO).

Welche Maßnahmen hierfür zu treffen sind, bestimmt sich nicht abstrakt, sondern nach einem beweglichen Maßstab: Unter Berücksichtigung des Standes der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ist ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO). Je höher das Risiko, desto anspruchsvoller sind die geschuldeten Maßnahmen.

Für ZaPuK fällt dieses Risiko hoch aus. Über die Infrastruktur werden dauerhaft und in großer Zahl Nachrichten mit teils höchstem Schutzbedarf übermittelt; nach der eigenen Einschätzung der Zielarchitektur kann die Korrelation der dabei anfallenden Daten bis zu Risiken für die nationale Sicherheit reichen (vgl. Metadatenreduktion). Der Maßstab des Art. 32 DSGVO ist an diesem hohen Schutzbedarf auszurichten.

b) Systemseitig-organisatorische und kryptografische Sicherung

Eine rein systemseitig-organisatorische Absicherung – etwa durch Zugriffskontrollen, ein Rollen- und Rechtemodell, Protokollierung und das Vier-Augen-Prinzip – ist grundsätzlich Bestandteil jedes Sicherheitskonzepts. Sie ist jedoch in erster Linie darauf gerichtet, eine unbefugte Veränderung nachträglich zu dokumentieren und aufzuklären, und weniger darauf, sie von vornherein zu verhindern oder für Dritte zweifelsfrei erkennbar zu machen. Bei einer verteilten Mehr-Betreiber-Infrastruktur, in der Daten Systemgrenzen und Vertrauensbereiche überschreiten, bleibt eine solche Absicherung lückenhaft, weil sie auf das Vertrauen in die jeweils verarbeitende Stelle angewiesen ist.

Kryptografische Verfahren – Signaturen, Siegel, Prüfsummen (Hashes) und versiegelte Zeitstempel – setzen demgegenüber unmittelbar am Datum an: Sie machen jede Veränderung erkennbar und erlauben den Nachweis der Unversehrtheit unabhängig davon, in wessen Machtbereich sich die Daten gerade befinden. Für ein am hohen Risiko orientiertes Schutzniveau nach Art. 32 DSGVO sind sie daher gegenüber der rein organisatorischen Absicherung sowohl wirksamer als auch – bei massenhafter Übermittlung schützenswerter Daten – dem Stand der Technik entsprechend. Zu beachten ist dabei, dass die Verschlüsselung als solche nur die Vertraulichkeit des Inhalts schützt und nicht bereits dessen Integrität oder Authentizität gewährleistet; die Integritätssicherung erfordert eigene Mechanismen und ist von der Verschlüsselung gedanklich zu trennen.

Die eingesetzten Verfahren müssen ihrerseits dem Stand der Technik entsprechen; als Orientierung dienen die einschlägigen Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) – insbesondere BSI TR-02102 – und der IT-Grundschutz. Weil sich der Stand der Technik fortlaufend verändert, ist zugleich eine Krypto-Agilität vorzusehen, die den Austausch der Verfahren ohne grundlegende Änderung der Anwendungslogik erlaubt (dazu ADR-1144).

c) Verhältnis zu den benachbarten Regelungsregimen (IT-Sicherheit, eIDAS)

Der Befund wird durch das IT-Sicherheitsrecht gestützt. Das mit der Umsetzung der NIS-2-Richtlinie neu gefasste BSIG verlangt in § 30 BSIG (für unter NIS-2 fallende Einrichtungen) Maßnahmen nach dem Stand der Technik und nennt in § 30 Abs. 2 Nr. 8 BSIG ausdrücklich „Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren" als Mindestmaßnahme; eine parallele Wertung enthält § 165 TKG für Telekommunikationsdienste. Zur Frage, ob und in welchem Umfang ZaPuK diesen Regimen unterfällt, siehe IV. Für die datenschutzrechtliche Beurteilung der Integritätssicherung nach Art. 32 DSGVO bestätigen diese Vorschriften jedenfalls, dass kryptografische Verfahren zum geschuldeten Standard gehören.

Hinzu kommt, dass kryptografische Mechanismen zwingend sind, soweit die eIDAS-VO eingreift. Für Dienste zur Zustellung elektronischer Einschreiben verlangt die eIDAS-VO die Sicherung gegen unbemerkte Veränderung durch fortgeschrittene bzw. qualifizierte Signaturen oder Siegel (Art. 44 Abs. 1 lit. d eIDAS-VO); die Integrität lässt sich dort nicht rein organisatorisch herstellen. Diese Anforderungen und die daran anknüpfende Vermutungswirkung werden im Zusammenhang mit der beweissicheren Übermittlung vertieft (siehe VII.1.3). Unabhängig davon erhöhen kryptografische Integritätsnachweise auch die prozessuale Beweiskraft elektronischer Dokumente und erleichtern der verantwortlichen Stelle die spätere Beweisführung.

Schließlich ist die Integrität vom bereits behandelten Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) und von der Authentizität zu unterscheiden: Die Richtigkeit betrifft die inhaltliche Korrektheit eines Datums, die Integrität dessen Unverändertheit und die Authentizität dessen belegbare Herkunft. Die kryptografischen Mechanismen von ZaPuK sichern Integrität und Authentizität, treffen aber keine Aussage über die sachliche Richtigkeit des Inhalts.

d) Übertragung auf ZaPuK

Die Zielarchitektur setzt die Integritätssicherung durchgängig kryptografisch und auf drei Ebenen um. Erstens wird die Integrität und Authentizität innerhalb des Kommunikationskanals durch die Ende-zu-Ende-Verschlüsselung des Matrix-Protokolls gegenüber den Kommunikationsparteien gewährleistet. Diese Sicherung wird bewusst unter Wahrung glaubhafter

Abstreitbarkeit realisiert und erzeugt daher keinen Beweis gegenüber Dritten (ADR-0012, ADR-0013). Zweitens wird die Integrität und Authentizität des Dokumenteninhalts gegenüber Dritten dadurch hergestellt, dass der Absender das Dokument vor dem Versand mit einem qualifizierten elektronischen Siegel bzw. einer qualifizierten Signatur versieht; Herkunft und Unversehrtheit sind damit auch außerhalb des Systems nachweisbar (ADR-0017). Drittens sichert die Bereitstellungsbestätigung die Integrität des Übermittlungsnachweises, indem sie einen kryptografischen Hash über das verschlüsselte Chiffrat der Nachricht bildet und diesen zusammen mit dem Eingangszeitpunkt mit dem Schlüssel des empfangenden Servers signiert (ADR-0018). Sämtliche Verfahren kommen ohne Zugriff auf den Klartext aus und sind damit mit der Ende-zu-Ende-Verschlüsselung vereinbar.

Diese Ausgestaltung entspricht dem hier entwickelten Maßstab: Nicht die rein organisatorische Dokumentation von Integritätsverletzungen, sondern deren kryptografische Verhinderung und Erkennbarkeit trägt das nach Art. 32 DSGVO gebotene Schutzniveau. Ergänzungsbedarf besteht im Wesentlichen bei den flankierenden Elementen – insbesondere bei der langfristigen Verifizierbarkeit der Nachweise (Vertrauensanker, qualifizierte Zeitstempel) und der Krypto-Agilität –, die in den PKI-Anforderungen konkretisiert werden (ADR-1144).

e) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Grundentscheidung, die Integrität nicht rein systemseitig-organisatorisch, sondern kryptografisch abzusichern, ist am Maßstab des Art. 32 DSGVO nicht nur zulässig, sondern angesichts des hohen Schutzbedarfs geboten. Eine allein auf Zugriffskontrollen, Protokollierung und Vier-Augen-Prinzip gestützte Absicherung wäre für ZaPuK nicht risikoangemessen.
- Die kryptografischen Mechanismen der Zielarchitektur (qualifiziertes Siegel des Inhalts nach ADR-0017, an das Chiffrat gebundene, signierte Bereitstellungsbestätigung nach ADR-0018, kryptografische Integrität im Kommunikationskanal nach ADR-0012 und ADR-0013) sind beizubehalten. Integrität, Authentizität und Richtigkeit sind dabei

auseinanderzuhalten; die kryptografische Sicherung leistet Integritäts- und Herkunftsnachweis, ersetzt aber keine inhaltliche Richtigkeitsprüfung.

- Die eingesetzten Verfahren sind am Stand der Technik auszurichten (BSI TR-02102, IT-Grundschutz) und krypto-agil auszugestalten, damit sie bei technologischem Fortschritt austauschbar bleiben; die langfristige Verifizierbarkeit der Nachweise ist über die PKI-Anforderungen sicherzustellen (ADR-1144).

- Der Maßstab des Standes der Technik ist mit dem IT-Sicherheitsrecht (§ 30 BSIG, § 165 TKG, ITSiV-PV) und – soweit einschlägig – mit den eIDAS-Anforderungen abzustimmen; eine doppelte Prüfung ist zu vermeiden, die bereichsspezifische Vertiefung erfolgt im IT-sicherheitsrechtlichen Teil und im Rahmen der beweissicheren Übermittlung (siehe IV).

3.6.2. Vertraulichkeit der Inhalte durch Verschlüsselung

a) Rechtliche (Un-)Verbindlichkeit der Ende-zu-Ende-Verschlüsselung im OZG-Kontext

Kurzzusammenfassung. Eine ausdrückliche gesetzliche Pflicht zur Ende-zu-Ende-Verschlüsselung besteht im OZG-Kontext nicht. Maßgeblich ist vielmehr der risikoangemessene Schutz nach dem Stand der Technik, wie ihn Art. 32 DSGVO und – für den Portalverbund – § 5 OZG in Verbindung mit der ITSiV-PV verlangen. Die Ende-zu-Ende-Verschlüsselung ist innerhalb dieses Rahmens keine zwingend vorgeschriebene, wohl aber eine besonders wirksame und deshalb vorzugswürdige Maßnahme zur Sicherung der Vertraulichkeit. Ihre rechtliche Verbindlichkeit im Einzelfall hängt davon ab, ob sie angesichts von Schutzbedarf und Bedrohungslage die einzige geeignete Stand-der-Technik-Maßnahme ist oder ob dieselben Risiken auch durch andere Maßnahmen (etwa eine qualifizierte Transportverschlüsselung mit flankierenden Vorkehrungen) angemessen behandelt werden können. Für ZaPuK ist die Ende-zu-Ende-Verschlüsselung angesichts der massenhaften und teils höchst sensiblen Kommunikation die datenschutz- und sicherheitsrechtlich vorzugswürdige und praktisch gebotene Ausgestaltung; ein Verzicht wäre allenfalls mit besonderer Begründung und wirksamen kompensierenden Maßnahmen

vertretbar. Perspektivisch kann die Ende-zu-Ende-Verschlüsselung durch Gesetz, Rechtsverordnung oder in Bezug genommene Technische Richtlinien des BSI ausdrücklich verbindlich gemacht werden.

aa) Kein ausdrückliches Verschlüsselungsgebot, aber ein risikobasierter Stand-der-Technik-Maßstab

Das OZG regelt die Bereitstellung von Verwaltungsleistungen über den Portalverbund sowie die Konten- und Postfachinfrastruktur, enthält aber kein ausdrückliches Gebot der Ende-zu-Ende-Verschlüsselung. Die Sicherheitsanforderungen werden nicht unmittelbar im Gesetz ausformuliert, sondern über Verweise und Verordnungsermächtigungen konkretisiert. Nach § 5 OZG werden die zur Gewährleistung der IT-Sicherheit erforderlichen Standards für die im Portalverbund und zu dessen Anbindung genutzten IT-Komponenten durch Rechtsverordnung des Bundesministeriums des Innern festgelegt. Deren Einhaltung ist für alle Stellen verbindlich, die entsprechende IT-Komponenten nutzen. Auf dieser Grundlage beruht die ITSiV-PV, die den Maßstab weiter konkretisiert: Nach § 2 Abs. 1 ITSiV-PV sind für den Portalverbund und die angebundenen IT-Komponenten Maßnahmen nach dem Stand der Technik zu treffen. Die Einhaltung dieses Standes wird nach § 2 Abs. 2 ITSiV-PV vermutet, wenn die in der Anlage aufgeführten Technischen Richtlinien des BSI eingehalten werden. IT-Sicherheit in diesem Sinne umfasst ausdrücklich die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen (§ 1 Abs. 3 ITSiV-PV).

Der so vorgegebene Maßstab deckt sich mit Art. 32 DSGVO, der ebenfalls ein am Stand der Technik und am Risiko orientiertes Schutzniveau verlangt und Verschlüsselung als grundsätzlich geeignete Maßnahme ausdrücklich hervorhebt (Art. 32 Abs. 1 lit. a DSGVO). Beide Regime führen zu demselben Ergebnis: Die Verschlüsselung ist eine – regelmäßig zentrale – Möglichkeit, das gebotene Schutzniveau zu erreichen, nicht aber die einzig zulässige. Die Auswahl der konkreten Maßnahmen bleibt Ergebnis einer risikobasierten Abwägung, in der die Ende-zu-Ende-Verschlüsselung als besonders wirksame Vertraulichkeitsmaßnahme allerdings ein erhebliches Gewicht hat.

bb) Ende-zu-Ende-Verschlüsselung als vorzugswürdige und bei hohem Schutzbedarf faktisch gebotene Maßnahme

Aus der Relativität des Stand-der-Technik-Maßstabs folgt, dass die Ende-zu-Ende-Verschlüsselung umso eher geboten ist, je höher der Schutzbedarf und je größer die Zahl der verarbeiteten Nachrichten ist. Wo – wie bei ZaPuK – eine bereichsübergreifende Infrastruktur massenhaft und teils höchst sensible Kommunikation abwickelt, verdichtet sich die Auswahl regelmäßig zugunsten der Ende-zu-Ende-Verschlüsselung: Sie muss bei der Maßnahmenauswahl Priorität genießen, weil mildere Maßnahmen das Risiko einer Kompromittierung zentraler Komponenten mit anschließender Korrelation von Inhalten und Metadaten nicht in gleicher Weise beherrschen. Für Konstellationen mit besonders hohem Schutzbedarf – etwa die Kommunikation von Teilnehmenden eines Zeugenschutzprogramms – wird eine Ende-zu-Ende-Verschlüsselung teilweise als zwingend angesehen.

Ein vollständiger Verzicht auf die Ende-zu-Ende-Verschlüsselung ist damit rechtlich nicht in jedem Fall ausgeschlossen, bei hohem Schutzbedarf aber nur bei nachvollziehbarer Begründung und mit hinreichenden kompensierenden Maßnahmen vertretbar. Die architekturprägende Grundentscheidung von ZaPuK für eine durchgängige Ende-zu-Ende-Verschlüsselung (ADR-0011, ADR-0012) ist vor diesem Hintergrund nicht nur zulässig, sondern die vorzugswürdige und praktisch gebotene Ausgestaltung. Sie entfaltet zugleich eine begrenzende Wirkung hinsichtlich der Anwendbarkeit des Datenschutzrechts: Für die reinen Transport- und Speicherakteure sind die verschlüsselten Inhalte mangels Schlüsselzugriffs nicht personenbezogen, sodass sich die Frage der Vertraulichkeitssicherung dort nicht mehr auf der Inhaltsebene stellt (siehe 1.3).

cc) Telekommunikationsrechtlicher Rahmen

Soweit ein ZaPuK-Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu V), treten die Vorgaben des TDDDG hinzu, die ihrerseits auf der ePrivacy-Richtlinie beruhen und nach Art. 95 DSGVO vorrangig sind, soweit sie dieselben Pflichten betreffen. Das Fernmeldegeheimnis nach § 3 TDDDG schützt Inhalt und nähere Umstände der Kommunikation und beschränkt die Kenntnisnahme durch die Verpflichteten auf das für die Diensterbringung

erforderliche Maß (§ 3 Abs. 3 TDDDG). Für Dienste mit Zwischenspeicherung verlangt § 6 Abs. 2 TDDDG technische und organisatorische Maßnahmen nach dem Stand der Technik, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten auszuschließen. Auch dieses Regime schreibt die Ende-zu-Ende-Verschlüsselung nicht ausdrücklich vor; seine Wertungen – Vertraulichkeit der Kommunikation und Begrenzung der Kenntnisnahme auf das Erforderliche – stützen jedoch die verschlüsselte Ausgestaltung. Umgekehrt stünde die Ende-zu-Ende-Verschlüsselung selbst dann, wenn Mitwirkungspflichten bei der Telekommunikationsüberwachung eingriffen, nicht generell in Frage, da die Verpflichteten nur die bei ihnen tatsächlich vorliegenden Daten in der vorhandenen Form auszuleiten haben.

dd) Neuere Rechtsentwicklung: sichere Übermittlungswege nach dem VwVfG

Die jüngste Änderung des Verwaltungsverfahrensgesetzes (siehe D.II.3.2.) bestätigt die Ausrichtung am Stand der Technik, ohne ein Verschlüsselungsgebot einzuführen. Das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern (BGBl. 2026 I Nr. 199) fasst die Vorschriften zur elektronischen Kommunikation neu und fügt einen § 3c VwVfG ein, der für sichere Übermittlungswege verlangt, dass sie auf einem dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruhen, die Identität der erklärenden Person festgestellt ist und sich diese zur Übermittlung authentisiert (§ 3c Abs. 1 VwVfG n.F.). Die näheren Festlegungen trifft eine Rechtsverordnung des Bundesministeriums des Innern (§ 3c Abs. 2 VwVfG n.F.). Die Vorschrift betrifft primär den Schriftformersatz (§ 3b VwVfG n.F.) und nicht unmittelbar die Vertraulichkeit der Inhalte. Sie zeigt aber, dass der Gesetzgeber auch im allgemeinen Verwaltungsverfahrensrecht auf am Stand der Technik ausgerichtete Protokollstandards setzt und deren Konkretisierung der Verordnungsebene überlässt. Diese Regelungstechnik – gesetzlicher Rahmen, Konkretisierung durch Rechtsverordnung – entspricht dem bereits im OZG angelegten Modell und eröffnet zugleich einen Hebel, über den künftig auch spezifische Verschlüsselungsanforderungen verbindlich gemacht werden könnten.

ee) Mögliche künftige Verbindlichkeit

Die Ende-zu-Ende-Verschlüsselung könnte auf mehreren Wegen ausdrücklich verbindlich vorgeschrieben werden: unmittelbar im Gesetz (etwa im OZG oder in einer spezialgesetzlichen

Grundlage für die Postfachinfrastruktur), durch Rechtsverordnung (insbesondere die ITSiV-PV oder eine Verordnung nach § 3c Abs. 2 VwVfG n.F.) oder mittelbar durch Fortschreibung der in der ITSiV-PV in Bezug genommenen Technischen Richtlinien des BSI, deren Einhaltung die Vermutung der Stand-der-Technik-Konformität begründet. In einem solchen Fall müssten Postfachinfrastrukturen die Ende-zu-Ende-Verschlüsselung zwingend unterstützen. Eine ausdrückliche Verankerung würde die derzeit auf einer Einzelfallabwägung beruhende Verbindlichkeit durch eine klare Vorgabe ersetzen und damit Rechtssicherheit schaffen.

ff) Folgerungen für die Architektur von ZaPuK

Die Grundentscheidung für eine durchgängige Ende-zu-Ende-Verschlüsselung (ADR-0011, ADR-0012) ist am Maßstab des Art. 32 DSGVO und des § 5 OZG in Verbindung mit § 2 ITSiV-PV nicht nur zulässig, sondern angesichts des hohen Schutzbedarfs die vorzugswürdige und praktisch gebotene Ausgestaltung.

Weil die Verbindlichkeit nach geltendem Recht das Ergebnis einer risikobasierten Abwägung ist, sollte die Wahl der Ende-zu-Ende-Verschlüsselung in der Schutzbedarfsfeststellung und im Sicherheitskonzept – flankierend in der Datenschutz-Folgenabschätzung – ausdrücklich begründet und dokumentiert werden. Dies belegt die Erforderlichkeit und trägt der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) Rechnung.

Die verbindliche Umsetzung gegenüber den teilnehmenden Stellen und Betreibern ist über die Anschlussbedingungen (ADR-1145) herzustellen, die die E2EE-Endpunkttreue und die sichere Ausgestaltung serverseitiger Entschlüsselungsendpunkte bereits adressieren.

Da der Stand der Technik dynamisch ist und die Ende-zu-Ende-Verschlüsselung künftig ausdrücklich vorgeschrieben werden kann, ist die Architektur krypto-agil zu halten (ADR-1144). Eine spezialgesetzliche oder verordnungsrechtliche Verankerung der Verschlüsselungsanforderung sollte – auch mit Blick auf § 3c Abs. 2 VwVfG n.F. und die ITSiV-PV – geprüft werden, um die derzeit kasuistische Beurteilung durch eine rechtssichere Vorgabe abzulösen.

b) Reichweite und Endpunkte der Ende-zu-Ende-Verschlüsselung

Kurzzusammenfassung. Wo die Ende-zu-Ende-Verschlüsselung terminiert, entscheidet nicht nur über das erreichte Sicherheitsniveau, sondern zugleich über die datenschutzrechtliche Einordnung der beteiligten Stellen. Der Terminierungspunkt bestimmt, wer Zugriff auf den Klartext erhält, und damit – nach dem relativen Maßstab des Personenbezugs (siehe 1.3) –, wer personenbezogene Inhaltsdaten verarbeitet und hierfür verantwortlich ist. Für die Einzelnutzer-Kommunikation terminiert die Verschlüsselung im Endgerät (ADR-1100); die reinen Backend-Betreiber verarbeiten hinsichtlich der Inhalte keine personenbezogenen Daten. Dies ist datenschutzrechtlich die vorzugswürdige Ausgestaltung.

Bei der Mehrbenutzer-Kommunikation (ADR-1101, ADR-1102) besteht ein Spannungsverhältnis zwischen der Vertraulichkeit und der Funktionalität von Funktionspostfächern, Vertretung und serverseitigen Diensten. Entscheidend ist, dass ein etwaiger zusätzlicher, serverseitiger Entschlüsselungsendpunkt im administrativen Machtbereich der empfangenden Organisation verbleibt: Ein dort betriebener technischer Nutzer ist kein Dritter im Sinne des Art. 4 Nr. 10 DSGVO, sondern eine unter der Verantwortung des Verantwortlichen befugte Stelle oder – bei Betrieb durch einen Dienstleister – ein Auftragsverarbeiter. Der Klartextzugriff im Machtbereich der Organisation bricht daher die datenschutzrechtlich geschützte Vertraulichkeit gegenüber Dritten nicht, sondern führt lediglich dazu, dass die Verarbeitung auf der Inhaltsebene der ohnehin verantwortlichen Organisation der DSGVO in vollem Umfang unterliegt. Die Terminierung außerhalb dieses Machtbereichs ist demgegenüber ausgeschlossen. Die Wahl zwischen den zulässigen Varianten ist eine risikobasierte Abwägung der verantwortlichen Stelle (d.h. der Organisation) nach Maßgabe der Schutzbedarfsfeststellung (Art. 25, Art. 32 DSGVO).

aa) Der Terminierungspunkt als Schlüssel für Anwendbarkeit und Verantwortlichkeit

Die Ende-zu-Ende-Verschlüsselung wirkt in der Zielarchitektur nicht nur als Sicherheitsmaßnahme, sondern zugleich als die Anwendbarkeit begrenzendes Gestaltungsmittel (siehe 1.3). Ob eine Stelle personenbezogene Inhaltsdaten verarbeitet, hängt davon ab, ob ihr der Klartext zugänglich ist; dies wiederum bestimmt der Punkt, an dem die Verschlüsselung endet. Die

Architekturentscheidungen zu den E2EE-Endpunkten sind daher nicht bloß technische Festlegungen, sondern bestimmen, welche Akteure als Verantwortliche oder Auftragsverarbeiter in der Pflicht stehen und welche – mangels Personenbezugs der ihnen vorliegenden Chiffrate – insoweit außerhalb des Anwendungsbereichs der DSGVO bleiben.

Maßstab bleibt der relative Begriff des Personenbezugs. Für einen Akteur, der lediglich das Chiffrat verarbeitet und die erforderlichen Schlüssel weder besitzt noch mit nach allgemeinem Ermessen wahrscheinlichen Mitteln erlangen kann, fehlt es hinsichtlich der Inhalte am Personenbezug. Dies entspricht der herrschenden Einordnung starker Verschlüsselung, wonach etwa bei der Ablage verschlüsselter Daten beim Cloud-Anbieter keine Offenlegung personenbezogener Daten vorliegt, solange dieser die Schlüssel nicht besitzt und sich nicht verschaffen kann; die Absicherung gegen einen Zugriff auf den Klartext muss dafür allerdings lückenlos gewährleistet sein. Genau diese Lückenlosigkeit ist der neuralgische Punkt der nachfolgend behandelten Endpunktentscheidungen.

bb) Einzelnutzer-Kommunikation: Terminierung im Endgerät (ADR-1100)

Für die Kommunikation einzelner Nutzender legt die Zielarchitektur fest, dass die Ver- und Entschlüsselung ausschließlich im Endgerät stattfindet und das private Schlüsselmaterial das Gerät nicht verlässt (ADR-1100, Option A). Diese Entscheidung ist datenschutzrechtlich nicht nur zulässig, sondern die vorzugswürdige Ausgestaltung. Sie bewirkt, dass die Betreiber der Postfach-Backends, der die Bereitstellungsbestätigung erzeugende Application Service und der Protokollkonverter hinsichtlich der Nachrichteninhalte keine personenbezogenen Daten verarbeiten (siehe 1.3). Zugleich verwirklicht sie den Datenschutz durch Technikgestaltung und die Sicherheit der Verarbeitung (Art. 25, Art. 32 Abs. 1 lit. a und b DSGVO) im höchstmöglichen Maß, weil die Vertraulichkeit der Inhalte gegenüber der Betriebsinfrastruktur strukturell und nicht bloß organisatorisch gesichert ist.

Die als Alternative erwogene Terminierung auf einem vorgelagerten Server außerhalb des Machtbereichs der nutzenden Person (ADR-1100, Option B) ist zu Recht ausgeschlossen worden. Ein solcher Server erhielte Zugriff auf den Klartext sämtlicher Nachrichten; sein Betreiber wäre – da er außerhalb des Verantwortungsbereichs der kommunizierenden Stellen stünde –

ein Dritter im Sinne des Art. 4 Nr. 10 DSGVO, dem die Inhalte offengelegt würden. Dies hebt den beschriebenen, die Anwendbarkeit des Datenschutzrechts begrenzenden Effekt auf, verlagert das gesamte Vertraulichkeitsrisiko auf eine einzelne, sicherheitskritische Komponente und widerspricht dem Zero-Trust-Ansatz. Der Ausschluss dieser Variante ist aus datenschutzrechtlicher Sicht folgerichtig.

cc) Mehrbenutzer-Kommunikation: der Machtbereich als Trennlinie (ADR-1101)

Bei Funktionspostfächern greifen mehrere Personen und technische Nutzer auf denselben verschlüsselten Nachrichtenbestand zu, dessen Mitgliederkreis sich über die Lebensdauer eines Vorgangs ändern kann. Die für die Einzelnutzer-Kommunikation ideale, ausschließlich in den Endgeräten terminierende Verschlüsselung lässt sich hier nicht ohne Weiteres mit den fachlichen Anforderungen an adressierbare Funktionspostfächer, automatisierte Vertretungsregelungen sowie serverseitige Dienste wie Archivierung und Schadsoftwareprüfung vereinbaren. Die Zielarchitektur löst diesen Zielkonflikt über abgestufte Terminierungsvarianten (ADR-1101). Datenschutzrechtlich sind diese danach zu beurteilen, ob der Klartext einem Dritten zugänglich wird oder im Machtbereich der empfangenden Organisation verbleibt.

Dies ergibt sich unmittelbar aus den Begriffsbestimmungen der DSGVO. Die empfangende Organisation ist bestimmungsgemäße Adressatin der Nachricht und damit Empfängerin im Sinne des Art. 4 Nr. 9 DSGVO, nicht Dritte. Dritter ist nach Art. 4 Nr. 10 DSGVO gerade nicht, wer unter der unmittelbaren Verantwortung des Verantwortlichen befugt ist, die Daten zu verarbeiten. Ein technischer Nutzer, der unter der administrativen Kontrolle der Organisation betrieben wird, ist deshalb kein Dritter. Wird er durch einen IT-Dienstleister betrieben, handelt dieser als Auftragsverarbeiter (Art. 28 DSGVO), ohne dass die Vertraulichkeit gegenüber Dritten berührt wäre. Der serverseitige Klartextzugriff im Machtbereich der Organisation ist damit datenschutzrechtlich kein Vertraulichkeitsbruch, sondern führt lediglich dazu, dass die Verarbeitung auf der Inhaltsebene der DSGVO in vollem Umfang unterliegt – bei einer Stelle, die für die inhaltliche Verarbeitung regelmäßig ohnehin verantwortlich ist (siehe 1.3 und 2.).

Vor diesem Hintergrund erweist sich die gewählte Grundvariante als tragfähig. Bei der Terminierung im Endgerät mit zusätzlichem technischem Nutzer im Machtbereich der Organisation

(ADR-1101, Option B) bleibt die Ende-zu-Ende-Verschlüsselung bis in die Endgeräte erhalten. Ein serverseitiger Klartextzugriff besteht nur in denjenigen Räumen, in denen der technische Nutzer als Teilnehmer geführt wird, und nur innerhalb des Verantwortungsbereichs der empfangenden Stelle. Gegenüber dem Betreiber der Infrastruktur und gegenüber Dritten bleibt die Vertraulichkeit gewahrt. Die Variante ist datenschutzrechtlich vertretbar, verlagert die Verantwortung für die serverseitig entschlüsselten Inhalte aber vollständig auf die Organisation, die diesen Endpunkt entsprechend abzusichern hat.

Für Kommunikation mit besonders hohem Schutzbedarf hält die Architektur zutreffend die Variante ohne serverseitigen Entschlüsselungsendpunkt bereit (ADR-1101, Option A). Wo das Schlüsselmaterial ausschließlich in den Endgeräten natürlicher Personen verbleibt, ist die Vertraulichkeit auch gegenüber der eigenen Organisation maximal gesichert. Diese Variante ist dort geboten, wo bereichsspezifische Geheimnisregime oder ein besonders hohes Risiko eine strikte innerorganisatorische Vertraulichkeit verlangen. Dies liegt in der Beurteilung des Verantwortlichen, kommt aber etwa im Anwendungsbereich des Sozialgeheimnisses (§ 35 SGB I), des Steuergeheimnisses (§ 30 AO), berufsrechtlicher Verschwiegenheitspflichten oder in Konstellationen wie dem Zeugenschutz in Betracht. Dass die Zielarchitektur diese Ausgestaltung als bedingte Alternative ausdrücklich ermöglicht, ist aus datenschutzrechtlicher Sicht hervorzuheben und beizubehalten.

Die Terminierung an der Organisationsgrenze (ADR-1101, Option C), bei der der gesamte vorgangsübergreifende Nachrichtenstrom an einem zentralen Punkt entschlüsselt wird, muss demgegenüber von der Organisation in eigener Verantwortlichkeit geprüft und begründet werden. Sie bricht die Ende-zu-Ende-Verschlüsselung zwischen den natürlichen Personen zwar nicht gegenüber Dritten, sofern der Terminierungspunkt im administrativen Machtbereich der empfangenden Stelle – einschließlich eines im Auftrag tätigen Dienstleisters – liegt. Sie ist datenschutzrechtlich jedoch mit einem gewissen Risiko verbunden, weil sie den Klartext einer Vielzahl von Vorgängen an einer Stelle konzentriert und damit sowohl unter dem Gesichtspunkt der Datensicherheit (Art. 32 DSGVO) als auch unter dem der Datenminimierung und der Begrenzung der Zugänglichkeit (Art. 5 Abs. 1 lit. c, Art. 25 Abs. 2 DSGVO) rechtfertigungsbedürftig ist. Die von der Zielarchitektur geforderte Beschränkung auf den Machtbereich der

empfangenden Stelle, die Begründungs- und Dokumentationspflicht sowie die Freigabe durch die verantwortliche Stelle sind daher sachgerecht.

Die Terminierung auf einem Server außerhalb des Machtbereichs der Organisation (ADR-1101, Option D) ist ausgeschlossen. Hier erhielte ein Dritter Zugriff auf den Klartext. Dies widerspricht sowohl der Vertraulichkeitsanforderung als auch dem relativen Personenbezug, der die Verschlüsselung überhaupt erst zu einem wirksamen Schutzinstrument macht. Der Ausschluss ist datenschutzrechtlich geboten.

dd) Vorgangsräume und Funktionspostfächer: Zugänglichkeitsbegrenzung und ihre Sicherung (ADR-1102)

Die Umsetzung der Funktionspostfächer über je Vorgang kryptografisch isolierte Räume (ADR-1102) verwirklicht die Datenminimierung in ihrer Ausprägung als Begrenzung der Zugänglichkeit, die Art. 25 Abs. 2 DSGVO ausdrücklich als Bezugsgröße nennt. Jeder Vorgang wird in einem eigenen Raum bearbeitet, externe Kommunikationspartner sehen ausschließlich ihren eigenen Vorgang, und der Zugriff der Bearbeitenden ergibt sich aus der Schlüsselverteilung und den über das Berechtigungsverzeichnis gesteuerten Mitgliedschaften. Diese Isolierung ist datenschutzrechtlich geboten und entspricht zugleich dem Need-to-Know-Prinzip, das die bereichsspezifischen Geheimnisregime ggf. auch innerorganisatorisch verlangen (etwa § 35 SGB I).

Die Konfiguration des technischen Nutzers – mit oder ohne Teilnahme an der Ende-zu-Ende-Verschlüsselung – ist eine Abwägung zwischen Verfügbarkeit und Vertraulichkeit und damit Gegenstand der Schutzbedarfsfeststellung (Art. 25, Art. 32 DSGVO). Nimmt der technische Nutzer an der Verschlüsselung teil, hält der Server das Schlüsselmaterial der ihm zugewiesenen Räume persistent vor. Dies erhöht die Angriffsfläche erheblich: Ein kompromittierter Server ermöglicht die – auch rückwirkende – Entschlüsselung der Kommunikation aller betroffenen Räume. Nach Art. 32 DSGVO sind daher Härtung, Zugriffsbeschränkung und Monitoring dieses Endpunkts geboten und die von der Architektur vorgesehene Möglichkeit, die Megolm-Session-Rotation auf kurze Intervalle zu konfigurieren, erscheint als risikomindernde Maßnahme sachgerecht. Wird der technische Nutzer demgegenüber ohne Teilnahme an der

Verschlüsselung oder die Raumverwaltung manuell durch Moderatoren betrieben, verringert sich das serverseitige Vertraulichkeitsrisiko. Dies geht allerdings zulasten der automatisierten Vertretung und des Zugriffs auf die Kommunikationshistorie und ist deshalb ebenfalls eine am Schutzbedarf auszurichtende Entscheidung.

Ergänzend tragen die Kennzeichnung des technischen Nutzers gegenüber den übrigen Teilnehmern und die revisionssichere Protokollierung administrativer Änderungen (ADR-1102) zur Transparenz und zur Rechenschaftsfähigkeit bei. Sie werden im Abschnitt zur Rechenschaftspflicht sowie – hinsichtlich der dabei anfallenden Protokolldaten – im Abschnitt zu den Logdaten aufgegriffen.

ee) Eigenverantwortung jeder Seite und Grenzen des Vertraulichkeitsversprechens

Die Dokumentation der geplanten Zielarchitektur weist zutreffend darauf hin, dass die Vertraulichkeit einer Kommunikation durch die schwächere Seite bestimmt wird und die sendende Partei nicht beeinflussen kann, wie die empfangende Seite die Nachricht nach dem Empfang verarbeitet (ADR-1101). Diese Feststellung hat eine datenschutzrechtliche Entsprechung: Jede beteiligte Stelle ist für die Verarbeitung in ihrer eigenen Sphäre eigenständig verantwortlich (siehe D.III.2.1.1.). Der Absender gibt mit der Ende-zu-Ende-Verschlüsselung kein über seine Sphäre hinausreichendes Vertraulichkeitsversprechen ab; er kann und muss lediglich sicherstellen, dass er den Klartext nur der bestimmungsgemäßen Empfängerseite zugänglich macht. Wie diese den Klartext innerhalb ihres Machtbereichs weiterverarbeitet – etwa im Rahmen einer Bearbeitungsvertretung, einer Archivierung oder einer Schadsoftwareprüfung –, liegt in ihrer eigenen Verantwortung und ist an den für sie geltenden Vorgaben zu messen. Für die architektonische Gestaltung folgt daraus, dass die Wahl der Terminierungsvariante der empfangenden Organisation zu überlassen und zugleich über die Anschlussbedingungen an die Wahrung des Machtbereichs zu binden ist.

ff) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Der Terminierungspunkt der Verschlüsselung ist zugleich der datenschutzrechtliche Prüfstein. Die Grundentscheidung, die Verschlüsselung für Einzelnutzer ausschließlich im Endgerät zu terminieren (ADR-1100), ist datenschutzrechtlich geboten. Sie sichert die Vertraulichkeit strukturell und hält die reinen Backend-Betreiber auf der Inhaltsebene aus dem Anwendungsbereich der DSGVO heraus.

- Maßgebliche Trennlinie für die Zulässigkeit eines serverseitigen Entschlüsselungsendpunkts ist der Verbleib im administrativen Machtbereich der empfangenden Organisation. Solange der technische Nutzer als befugte Stelle (Art. 4 Nr. 10 DSGVO) oder als Auftragsverarbeiter (Art. 28 DSGVO) innerhalb dieses Machtbereichs betrieben wird, liegt keine Offenlegung an Dritte vor. Die gewählte Variante B (ADR-1101) erscheint auf dieser Grundlage vertretbar. Variante D bleibt ausgeschlossen.

- Die Möglichkeit, für besonders schützenswerte Kommunikation ohne serverseitigen Endpunkt zu arbeiten (ADR-1101, Option A), ist beizubehalten. Für Verarbeitungen unter besonderen Geheimnisregimen (§ 35 SGB I, § 30 AO, Berufsgeheimnisse) und bei sehr hohem Schutzbedarf ist dies eine ggf. notwendige Gestaltung (was von der Organisation in eigener Verantwortung zu beurteilen ist).

- Die Entscheidung für eine Terminierung an der Organisationsgrenze (Option C) sollte jeweils begründet werden. Die Begründungs-, Dokumentations- und Freigabepflicht sowie die Bindung an den Machtbereich der empfangenden Stelle sind aufrechtzuerhalten. Ergänzend ist zu empfehlen, einen Migrationspfad hin zu Variante B vorzusehen.

- Die kryptografische Isolierung je Vorgang und die berechtigungsgesteuerte Zugänglichkeit (ADR-1102) verwirklichen Art. 25 Abs. 2 DSGVO und das Need-to-Know-Prinzip und sind konsequent umzusetzen.

- Nimmt der technische Nutzer an der Verschlüsselung teil, ist der Server sicherheitskritisch. Härtung, Zugriffsbeschränkung, Monitoring und eine risikoangemessene

Schlüsselrotation sind nach Art. 32 DSGVO zwingend und sollten über die Anschlussbedingungen (ADR-1145) verbindlich gemacht werden.

- Die Wahl der Terminierungsvariante obliegt der empfangenden Organisation auf Grundlage ihrer Schutzbedarfsfeststellung. Sie ist zu dokumentieren und sollte über die Anschlussbedingungen an die Wahrung des administrativen Machtbereichs gebunden werden, ohne die eigenständige datenschutzrechtliche Verantwortung der jeweiligen Stelle zu verlagern.

c) Serverseitige Verarbeitung: Malware-Prüfung unter Ende-zu-Ende-Verschlüsselung

Kurzzusammenfassung. Der Schutz vor Schadsoftware ist ein berechtigtes und nach Art. 32 DSGVO gefordertes Sicherheitsziel, das der Integrität und der Verfügbarkeit der Verarbeitung dient. Die Zielarchitektur greift es mit der Anforderung SIC_ÜBE_MAL_005 und mit ADR-1130 auf. Eine Prüfung auf Schadinhalte setzt jedoch den Zugriff auf den Klartext voraus und ist deshalb nur dort möglich, wo der Klartext tatsächlich vorliegt, nämlich an den Endpunkten der Verschlüsselung. Bei strikter Ende-zu-Ende-Verschlüsselung ist eine serverseitige Inhaltsprüfung auf der Transportstrecke ausgeschlossen, weil eine Ende-zu-Ende-Verschlüsselung und ein serverseitiger Zugriff auf den Nachrichtenklartext einander begrifflich ausschließen. Umgekehrt besteht keine Rechtspflicht zu einer zentralen, serverseitigen Inhaltsprüfung; die Malware-Prüfung darf vollständig auf die Endgeräte oder in den Machtbereich der empfangenden Stelle verlagert werden. Weder die DSGVO noch die ITSiV-PV verlangen eine zentrale Inhaltskontrolle; das Fernmeldegeheimnis (§ 3 Abs. 3 TDDDG) und die grundrechtlich geschützte Vertraulichkeit der Kommunikation sprechen im Gegenteil gerade gegen eine über das Erforderliche hinausgehende Kenntnisnahme durch den Betreiber. Die von ZaPuK gewählte Kombination aus Endgeräteschutz, organisationsseitiger Prüfung an einem serverseitigen E2EE-Endpunkt und SDK-gestützter Delegation an einen im Machtbereich betriebenen Scandienst (ADR-1130) ist damit datenschutz- und sicherheitsrechtlich tragfähig. Der Verzicht auf einen zentralen, den Klartext prüfenden Dienst ist folgerichtig.

aa) Ausgangspunkt: Malware-Schutz als Sicherheitsziel und die Grenze der Verschlüsselung

Der Schutz vor Schadsoftware gehört zu den Maßnahmen, mit denen der Verantwortliche die Integrität und Verfügbarkeit der Systeme und der verarbeiteten Daten auf Dauer sicherzustellen hat (Art. 32 Abs. 1 lit. b DSGVO). Er ist Bedingung für das zu gewährleistende risikoangemessene Schutzniveau und wird auch durch das IT-Sicherheitsrecht gefordert, das u.a. die Bewältigung von Sicherheitsvorfällen ausdrücklich zu den Mindestmaßnahmen zählt (§ 30 Abs. 2 BSIG). Beide Regime stellen zudem Verschlüsselung als wesentliche Maßnahme zur Gewährleistung der Vertraulichkeit heraus. Daraus entsteht ein Zielkonflikt: Während die Ende-zu-Ende-Verschlüsselung die Vertraulichkeit maximiert, verlangt der Malware-Schutz einen Zugriff auf den unverschlüsselten Inhalt. Eine Prüfung ist ihrer Natur nach nur am Klartext möglich und damit nur an einem E2EE-Endpunkt zu leisten. Die Auflösung dieses Konflikts ist keine Frage des Ob des Malware-Schutzes, sondern des Wo seiner Durchführung.

bb) Unzulässigkeit einer serverseitigen Inhaltsprüfung unter strikter E2EE

Das Postfach-Backend und die übrigen reinen Transport- und Speicherakteure verarbeiten die Nachrichteninhalte nur als Chiffrat. Da ihnen der Schlüssel und damit der Zugriff auf den Klartext fehlt, ergeben sich aus dieser Architekturentscheidung vor dem Hintergrund des relativen Personenbezugs erhebliche Vorteile in der datenschutzrechtlichen Betrachtung (siehe 1.3).

Ein echter Malware-Scan des Nachrichteninhalts auf der Transportstrecke wäre nur um den Preis zu haben, die Ende-zu-Ende-Verschlüsselung aufzubrechen oder einem Zwischenakteur den Schlüssel zugänglich zu machen (eine bloße Mustererkennung im Chiffrat, wie sie etwa homomorphe Verfahren erlauben, kann eine inhaltliche Schadcodeprüfung nicht ersetzen). Die Festlegung auf eine strikte Ende-zu-Ende-Verschlüsselung richtet sich aber gerade dagegen, dass der Serverbetreiber oder ein sonstiger Dritter die Inhalte in irgendeiner Form verarbeiten kann. Ein inhaltlicher Zugriff des Betreibers zum Zweck der Prüfung würde die anwendbarkeitsbegrenzende Wirkung der Verschlüsselung aufheben (siehe 1.3), den Betreiber zur für die Inhalte verantwortlichen Stelle machen und ein Konzentrationsrisiko schaffen, welches die Ende-zu-Ende-Verschlüsselung vermeiden soll. Dies würde im Widerspruch zur

Vertraulichkeitsanforderung der Zielarchitektur (SIC_VER_ÜBE_032) stehen und mit Blick auf die rechtlichen Vertraulichkeitsanforderungen (u.a. Art. 32 DSGVO, § 30 BSIG) einen erheblichen Begründungsaufwand verursachen. Dass die alternative erwogene Prüfung im Content-Repository des Homeservers ausgeschlossen wurde (ADR-1130, Option A), steht daher im Einklang mit den rechtlichen Anforderungen.

cc) Zulässigkeit der Verlagerung auf die Endgeräte und den Machtbereich

Spiegelbildlich dazu, dass die serverseitige Inhaltsprüfung problematisch bis unzulässig ist, erscheint die vollständige Verlagerung der Malware-Prüfung auf die Endgeräte oder in den Machtbereich der empfangenden Stelle rechtlich zulässig. Eine Pflicht der Betreiber zur serverseitigen Entschlüsselung und Prüfung besteht nicht. Weder die DSGVO noch die ITSiV-PV verlangen eine zentrale Inhaltskontrolle. Das Fernmeldegeheimnis untersagt es den Verpflichteten sogar, sich über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt der Kommunikation zu verschaffen (§ 3 Abs. 3 TDDDG).

Die somit verbleibende Möglichkeit der dezentralen Prüfung, die den Betreiberzugriff auf die Inhalte vermeidet, ist damit nicht nur zulässig, sondern entspricht der Wertung des Kommunikationsdatenschutzes. Sie findet zugleich Rückhalt in den einschlägigen Grundrechten und grundrechtsgleichen Gewährleistungen, namentlich im Fernmeldegeheimnis des Art. 10 GG, im Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie in Art. 7 und Art. 8 EU-Grundrechtcharta und Art. 8 EMRK. Sie sprechen für Lösungen, die die Ende-zu-Ende-Verschlüsselung mit einer Schlüsselhoheit bei den Endnutzern verwirklichen.

Findet die Prüfung nicht auf dem Endgerät selbst, sondern durch Übergabe des entschlüsselten Inhalts an einen Scandienst statt (ADR-1130, Optionen D und E), ist datenschutzrechtlich entscheidend, dass dieser Dienst im Machtbereich der prüfenden Stelle verbleibt. Ein im administrativen Machtbereich der Organisation betriebener technischer Nutzer, der als E2EE-Teilnehmer den Klartext prüft, ist kein Dritter im Sinne des Art. 4 Nr. 10 DSGVO, sondern eine befugte Stelle oder, bei Betrieb durch einen IT-Dienstleister, ein Auftragsverarbeiter; die Prüfung an diesem Endpunkt bricht die datenschutzrechtlich geschützte Vertraulichkeit gegenüber Dritten

nicht (siehe b)). Die Übergabe des Klartextes an einen zentralen, außerhalb des Machtbereichs betriebenen Scanner ist demgegenüber nur auf freiwilliger, einwilligungsgestützter Grundlage vertretbar und darf nicht zum Regelweg werden.

dd) Exkurs: Verhältnis von Malware-Prüfung und Chatkontrolle

Von der hier beschriebenen endpunktbasierten Malware-Prüfung ist die auf Unionsebene diskutierte fremdnützige Inhaltsdurchsuchung zu unterscheiden, wie sie im Umfeld der Verordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern („Chatkontrolle") erörtert wird. Zwar setzt das dort diskutierte Client-Side-Scanning wie die hier betrachtete Malware-Prüfung am Endgerät an. Jedoch ergeben sich aus dem Zweck und dem Außenbezug der Verarbeitung ganz wesentliche Unterschiede. Die Malware-Prüfung dient dem Schutz des Empfängers an dem ihm ohnehin zugänglichen Klartext, steht unter seiner Kontrolle und meldet ihr Ergebnis nicht nach außen. Eine anlasslose Durchsuchung des Inhalts gegen extern vorgegebene Kriterien mit anschließender Meldung an eine dritte Stelle würde demgegenüber das Vertraulichkeitsversprechen der Ende-zu-Ende-Verschlüsselung aushöhlen und wäre grundrechtlich bedenklich. Zu trennen sind dabei aktuell zwei EU-Rechtsakte: Die bis 2028 verlängerte befristete Verordnung (EU) 2021/1232 erlaubt Anbietern lediglich ein freiwilliges Scannen unverschlüsselter Kommunikation und lässt die Ende-zu-Ende-Verschlüsselung ausdrücklich unberührt. Die dauerhafte CSA-Verordnung (Vorschlag COM(2022) 209) mit ihren verpflichtenden Aufdeckungsanordnungen befindet sich derzeit im Trilog und ist somit derzeit nicht in Kraft. Für ZaPuK ist maßgeblich, dass keine geltende Vorschrift eine fremdnützige Inhaltsdurchsuchung erzwingt. Aus grundrechtlicher Perspektive sollte die Architektur derartige Mechanismen auch nicht vorsehen.

ee) Das De-Mail-Gegenmodell und seine Ablösung

Die Grenzen einer serverseitigen Prüfung lassen sich am Beispiel von De-Mail nachzeichnen, das bewusst den entgegengesetzten Weg gegangen ist. Das De-Mail-G verzichtet auf eine zwingende Ende-zu-Ende-Verschlüsselung gerade deshalb, um dem akkreditierten Diensteanbieter eine Prüfung der Nachrichten auf Schadsoftware zu ermöglichen. Die Freischaltung des Kontos setzt die Einwilligung des Nutzers in eine solche Prüfung voraus (§ 3 Abs. 4 Nr. 4 De-

Mail-G), und die technischen Vorgaben des BSI machten sie zur Voraussetzung der Akkreditierung. Zugleich bleibt eine durchgängige Verschlüsselung zwischen Sender und Empfänger nach dem Gesetz ausdrücklich unberührt (§ 5 Abs. 3 Satz 3 De-Mail-G) – mit der Folge, dass eine tatsächlich Ende-zu-Ende-verschlüsselte Nachricht der providerseitigen Prüfung gerade entzogen ist. Im Behördenkontakt wurde die Verschlüsselung dementsprechend regelmäßig nicht bis zum Endgerät, sondern nur bis zum Gateway der Behörde geführt. Flankierend stellten § 30 Abs. 7 AO und § 87a Abs. 1 Satz 5 AO klar, dass die kurzzeitige automatisierte Entschlüsselung durch den akkreditierten Diensteanbieter zum Zweck der Schadsoftwareprüfung und der Weiterleitung keine unbefugte Offenbarung des Steuergeheimnisses und keinen Verstoß gegen das Verschlüsselungsgebot darstellt.

Dieses Modell wird gegenwärtig abgewickelt. Das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern (BGBl. 2026 I Nr. 199) streicht sowohl § 30 Abs. 7 AO als auch § 87a Abs. 1 Satz 5 AO und ordnet das Außerkrafttreten des De-Mail-G mit Ablauf des 31. Dezember 2026 an (§ 26 De-Mail-G n.F.). Die gesetzliche Privilegierung der providerseitigen Entschlüsselung zu Prüfzwecken entfällt damit ebenso wie der Trägerdienst, an den sie anknüpfte. Diese Entwicklung steht im Einklang mit dem Ansatz von ZaPuK, das Modell einer zentralen, den Klartext prüfenden Instanz nicht fortzuschreiben, sondern durch endpunktbasierte Lösungen abzulösen.

ff) Übertragung auf ZaPuK (ADR-1130)

Die Zielarchitektur löst den beschriebenen Zielkonflikt nicht durch eine einzige Maßnahme, sondern durch eine an den jeweiligen E2EE-Endpunkt anknüpfende Kombination. Bei Organisationen mit Funktionspostfächern kann ein technischer Nutzer als E2EE-Teilnehmer den entschlüsselten Anhang prüfen, bevor er an die Bearbeitenden verteilt wird. Die Prüfung findet dann am serverseitigen Endpunkt im Machtbereich der Organisation statt (ADR-1130 in Verbindung mit ADR-1101, Option B). Für Privatpersonen sowie für Organisationen ohne serverseitigen Entschlüsselungsendpunkt erfolgt die Prüfung auf dem Endgerät durch die dort installierte Schutzsoftware. Das ZaPuK-SDK kann diese Prüfung unterstützen, indem es die entschlüsselten Inhalte an die Schnittstellen des Betriebssystems oder an einen im Machtbereich

betriebenen Scandienst delegiert (ADR-1130, Optionen B und E). Ein zentraler, den Klartext prüfender Dienst ist demgegenüber ausgeschlossen; ein zentraler Malware-Scanner (Option D) kommt allenfalls freiwillig und nach vorheriger Zustimmung der Nutzenden in Betracht.

Diese Ausgestaltung ist datenschutz- und IT-sicherheitsrechtlich folgerichtig. Sie hält die Ende-zu-Ende-Verschlüsselung ausnahmslos ein und verlagert die Prüfung an die Orte, an denen sie rechtlich zulässig und technisch möglich ist. Zu benennen bleibt der damit verbundene, hinzunehmende Umstand, dass sich unter Wahrung strikter Ende-zu-Ende-Verschlüsselung kein einheitliches Schutzniveau erreichen lässt: Die Qualität der Prüfung hängt vom jeweiligen Endgerät und Betriebsmodell ab, und Privatpersonen ohne aktuelle Endgeräteschutzlösung bleiben ungeschützt. Dieses Restrisiko ist Ausdruck der bewussten Priorisierung der Vertraulichkeit (Architekturkonzept, Abschnitt 2.3, KAP-3) und lässt sich nicht auflösen, ohne den Klartext an eine zentrale Stelle zu geben und damit die Vertraulichkeit preiszugeben. Es ist daher als Ergebnis einer risikobasierten Abwägung tragfähig. Abgesichert werden kann die Prüfung über die Anschlussbedingungen, die Organisationen verpflichten können, an einem ihrer E2EE-Endpunkte oder über einen Scandienst eine Malware-Prüfung durchzuführen (ADR-1145).

gg) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Der Ausschluss einer serverseitigen Inhaltsprüfung im Content-Repository (ADR-1130, Option A) erscheint datenschutz- und IT-sicherheitsrechtlich geboten. Eine echte Malware-Prüfung des Klartextes durch einen reinen Transport- oder Speicherakteur wäre mit der strikten Ende-zu-Ende-Verschlüsselung (SIC_VER_ÜBE_032) und aus rechtlicher Sicht mit dem Fernmeldegeheimnis (§ 3 Abs. 3 TDDDG) unvereinbar.
- Die vollständige Verlagerung der Prüfung auf die Endgeräte und in den Machtbereich der empfangenden Stelle ist zulässig. Eine Rechtspflicht zur zentralen Inhaltskontrolle besteht nicht; die dezentrale Lösung entspricht dem Kommunikationsdatenschutz und der grundrechtlich geschützten Vertraulichkeit.

- Prüfungen an einem serverseitigen E2EE-Endpunkt (technischer Nutzer) oder durch einen delegierten Scandienst sind nur zulässig, solange sie den administrativen Machtbereich der empfangenden Stelle nicht verlassen. Der dortige Zugriff auf den Klartext begründet keine Offenlegung an Dritte, unterstellt die Verarbeitung aber vollständig der DSGVO. Ein zentraler externer Scan-Service sollte auf freiwillige, einwilligungsgestützte Nutzung beschränkt werden.

- Das De-Mail-Modell der providerseitigen Entschlüsselung zu Prüfzwecken ist mit der Streichung von § 30 Abs. 7 AO und § 87a Abs. 1 Satz 5 AO sowie dem Außerkrafttreten des De-Mail-G zum 31. Dezember 2026 überholt und sollte schon deshalb nicht als Vorbild dienen.

- Das unter strikter Ende-zu-Ende-Verschlüsselung unvermeidbar uneinheitliche Schutzniveau ist als verbleibendes hinzunehmendes Risiko zu dokumentieren. Die Pflicht zur Malware-Prüfung an einem E2EE-Endpunkt sollte über die Anschlussbedingungen (ADR-1145) verbindlich gemacht werden, ohne die eigenständige Verantwortung der teilnehmenden Stelle zu verlagern.

d) Archivierung und Stellvertretung

Kurzzusammenfassung. Archivierung und Stellvertretung sind die beiden praktischen Anwendungsfälle, in denen ein anderer als der ursprüngliche Empfänger auf verschlüsselte Inhalte zugreifen können muss. Ob dies mit der Ende-zu-Ende-Verschlüsselung vereinbar ist, hängt technisch davon ab, wo deren Endpunkt liegt: Terminiert die Verschlüsselung ausschließlich im Endgerät der handelnden natürlichen Person (nutzerzentrisch), sind Archivierung und automatisierte Vertretung kaum umsetzbar; verlagert man den Endpunkt in den Machtbereich der Organisation (rollen- oder organisationszentrisch), werden sie möglich, ohne dass die datenschutzrechtlich geschützte Vertraulichkeit gegenüber Dritten aufgegeben wird. Rechtlich maßgeblich ist die bereits entwickelte Betrachtung des Machtbereichs der empfangenden Stelle (bzw. Organisation): Ein technischer Nutzer oder ein Archivsystem im administrativen Machtbereich des Empfängers ist kein Dritter im Sinne des Art. 4 Nr. 10 DSGVO, sondern eine befugte Stelle oder – bei Betrieb durch einen Dienstleister – ein Auftragsverarbeiter.

Das eigentliche datenschutzrechtliche Problem betrifft daher nicht die Transportinfrastruktur, sondern liegt innerhalb der nutzenden Organisation (innerorganisatorische Vertraulichkeit, Need-to-know). Die Zielarchitektur trägt dem zutreffend Rechnung: Die Aufbewahrung erfolgt im Machtbereich der jeweils verantwortlichen Stelle statt in einem zentralen Dienst (ADR-1135), die Bearbeitungsvertretung wird über kryptografisch isolierte Vorgangsräume und ein Berechtigungsverzeichnis abgebildet (ADR-1102, ADR-1112), und für die externe Bevollmächtigung sowie die gesetzliche Vertretung handelt die vertretende Person mit eigener Identität und übermitteltem Vertretungsnachweis, ohne fremden Postfachzugriff (ADR-1113). Die abschließende Wahl zwischen den Terminierungsvarianten obliegt der Organisation auf Grundlage ihrer Schutzbedarfsfeststellung (Art. 25, Art. 32 DSGVO). Für die zeitliche Dimension (Lösch- und Aufbewahrungsfristen, Archivrecht) wird auf den Abschnitt zur Speicherbegrenzung verwiesen (siehe 3.5.1).

aa) Die Definition von „Ende-zu-Ende“ ist entscheidend für die Umsetzbarkeit

Archivierung und Stellvertretung werden für die Ende-zu-Ende-Verschlüsselung dasselbe Problem auf: Beide verlangen, dass jemand anderes auf einen Inhalt zugreifen kann, der ursprünglich nur für eine bestimmte Person bestimmt war. Ob dies unter Wahrung der Ende-zu-Ende-Verschlüsselung gelingt, hängt davon ab, was im jeweiligen Kontext als „Ende“ der Verschlüsselung definiert wird.

Insoweit lassen sich drei Spielarten unterscheiden, die sich im Schutzniveau und in ihrer Eignung für Archivierung und Vertretung unterscheiden: Bei der nutzerzentrischen Verschlüsselung liegt der Endpunkt allein im Endgerät der handelnden natürlichen Person; nur diese verfügt über den privaten Schlüssel. Diese Variante maximiert den Schutz – auch vor Innentätern – und deckt damit selbst sehr hohen Schutzbedarf ab, erschwert aber Vertretung und Archivierung erheblich, weil außer der zuständigen Person niemand entschlüsseln kann. Bei der rollenzentrischen Verschlüsselung erfolgt die Entschlüsselung zusätzlich über einen Rollen- bzw. Funktionsschlüssel innerhalb der Organisation, der Teamarbeit, Vertretung und Archivierung ermöglicht, das innerorganisatorische Risiko aber erhöht. Bei der organisationszentrischen

Verschlüsselung ist die Organisation selbst der Endpunkt, was die größte Flexibilität, aber auch die größte Konzentration von Klartext an einer Stelle bedeutet.

Eine kanonische Definition von „E2EE" existiert nicht; technische Referenzen bestimmen den Endpunkt unterschiedlich weit. Teils ist die Bestimmung des Endpunkts sehr offen gehalten, etwa als „final destination" (IETF, RFC 4949).[277] Das BSI stellt in der TR-03190 ausdrücklich auf die Organisation beziehungsweise den in ihrem Verantwortungsbereich betriebenen Anschlussknoten ab.[278] Bemerkenswert ist, dass die zuletzt genannte amtliche Referenz einen serverseitigen Entschlüsselungsendpunkt im Verantwortungsbereich der Stelle – an dem der Klartext entschlüsselt und geprüft wird – ausdrücklich noch als „Ende-zu-Ende-Verschlüsselung" begreift. Dies stützt das hier zugrunde gelegte Abstellen auf den Machtbereich der Empfängerorganisation.

Die genannte Abstufung entspricht unmittelbar den Terminierungsvarianten der Zielarchitektur: Der nutzerzentrischen Verschlüsselung entspricht Option A des ADR-1101 (E2EE ohne Automatisierung), der rollenzentrischen die dort gewählte Option B (technischer Nutzer als E2EE-Teilnehmer), der organisationszentrischen die als begründete Ausnahme zugelassenen Option C (Terminierung an der Organisationsgrenze). Wie im Abschnitt b) dargelegt, ist für die datenschutzrechtliche Beurteilung nicht entscheidend, dass an einem dieser Endpunkte Klartext anfällt, sondern allein, dass der Endpunkt den administrativen Machtbereich der empfangenden Stelle nicht verlässt. Der Zielkonflikt zwischen der Vertraulichkeit einerseits und der Verfügbarkeit für Archivierung und Vertretung andererseits ist damit – per Definition – keine Frage des Ob der E2EE, sondern eine Abwägungsentscheidung über die Lage ihres Endpunkts, die der jeweiligen Organisation nach Maßgabe ihrer Schutzbedarfsfeststellung obliegt (Art. 25, Art. 32 DSGVO).

[277] IETF, RFC 4949, Internet Security Glossary, Version 2 (2007), Stichwort „end-to-end encryption": Entschlüsselung erst an der „final destination"; in der IT-sicherheitswissenschaftlichen Rezeption vielfach als „intended final destination" zitiert (etwa Demjaha u. a., USEC 2018).

[278] BSI, Technische Richtlinie TR-03190, IT-Sicherheitsanforderungen für die Anbindung an das NOOTS, Version 1.0 (25.03.2026), Kap. 2 (Begriffsdefinitionen), S. 10: „Die „Enden der Verschlüsselung" liegen in den Sicheren Anschlussknoten, die im Verantwortungsbereich der sendenden bzw. empfangenden Stelle betrieben werden und den entschlüsselten Inhalt prüfen".

bb) Archivierung unter Ende-zu-Ende-Verschlüsselung

Die datenschutzrechtliche Zulässigkeit der Aufbewahrung als solche – insbesondere das Verhältnis von Löschpflicht (Art. 5 Abs. 1 lit. e, Art. 17 DSGVO) und Aufbewahrungs- bzw. Archivrecht (§ 6a EGovG, §§ 5, 6 BArchG) sowie die Archivprivilegierung des Art. 5 Abs. 1 lit. b in Verbindung mit Art. 89 DSGVO – ist im Abschnitt zur Speicherbegrenzung behandelt (siehe 3.5.1). Im Folgenden geht es um die Frage, wie sich die Übernahme in Archiv- und E-Akte-Systeme technisch-organisatorisch mit der durchgängigen Verschlüsselung vereinbaren lässt.

Eine Archivierung kann nur dort ansetzen, wo der Klartext vorliegt, also an einem Endpunkt der Verschlüsselung. Die Zielarchitektur sieht konsequent keinen zentralen Aufbewahrungsdienst vor, sondern belässt die Veraktung und Archivierung im Machtbereich der jeweiligen Datenbesitzer (ADR-1135). Die Übernahme erfolgt entweder über das Endgerät oder – regelbasiert für alle Vorgänge eines Funktionspostfachs – über einen technischen Nutzer, der als E2EE-Teilnehmer am Vorgangsraum teilnimmt. Diese Verortung ist datenschutzrechtlich nicht nur zulässig, sondern geboten: Sie weist die revisionssichere Langzeitsicherung der ohnehin dafür zuständigen behördlichen Sphäre zu und vermeidet zugleich eine zentrale Konzentration von Inhalten und Metadaten, die als eigenständiges Sicherheitsrisiko zu bewerten wäre. Dass der als Alternative erwogene zentrale Aufbewahrungsdienst (ADR-1135, Option B) demgegenüber zurückgestellt wurde, erscheint aus datenschutzrechtlicher Sicht konsequent, da er entweder Metadaten an zentraler Stelle anhäufen oder ein für alle Teilnehmer tragfähiges zentrales Schlüsselmanagement voraussetzen würde.

Technisch stehen für die rollen- und organisationszentrischen Varianten etablierte Mittel zur Verfügung. Für die E-Akte kommt ein behördlicher Journal- bzw. Archivschlüssel in Betracht; die Nachricht wird dann für die verschiedenen berechtigten Empfängerschlüssel mehrfach verschlüsselt, sodass neben den handelnden Personen auch das Archivsystem entschlüsseln kann, ohne dass die Verschlüsselung gegenüber Dritten aufgegeben würde. In der Umsetzung der Zielarchitektur übernimmt diese Funktion der als E2EE-Teilnehmer konfigurierte technische Nutzer, der die Session-Schlüssel des Vorgangsraums hält und an die Übernahmekomponente weiterreichen kann (ADR-1101, ADR-1102). Das dabei erzeugte Exportpaket (ADR-1135)

umfasst neben Nachricht und Anhängen die zugehörigen Nachweisartefakte – Identitätsnachweis, Bereitstellungsbestätigung, gegebenenfalls Abruf- oder Lesebestätigung sowie Siegel oder Signatur – und sichert damit die Beweiskette über den Kommunikationskanal hinaus. Wo eine solche automatisierte Übernahme aus Vertraulichkeitsgründen unterbleibt (nutzerzentrische Variante), verbleibt die Archivierung bei der clientseitigen, vorgangsbezogenen Ausleitung; dies ist im Betriebsmodell A der einzige Weg (ADR-1135).

Datenschutzrechtlich ist zweierlei zu beachten: Erstens gilt auch für die archivierten Bestände der Grundsatz, dass eine bloß abstrakte künftige Nützlichkeit eine Vorhaltung „auf Vorrat" nicht trägt. Die Erforderlichkeit der fortgesetzten Speicherung muss sich hinreichend konkretisiert haben oder auf einer Aufbewahrungs- bzw. Archivierungspflicht beruhen.[279] Zweitens ist der Kreis der Zugriffsberechtigten auch im Archiv auf das erforderliche Maß zu begrenzen (Art. 5 Abs. 1 lit. c, Art. 25 Abs. 2 DSGVO). Wo eine dauerhafte, aber streng zugriffsbeschränkte Vorhaltung gefordert ist, kann – als Referenzmodell für besonders sensible Bestände – die Einschaltung eines Datentreuhänders erwogen werden, der den Zugriff nur in eng umgrenzten, vorab festgelegten Fällen und Verfahren freigibt.[280] Für ZaPuK folgt daraus, dass die Konfigurierbarkeit differenzierter Aufbewahrungs- und Zugriffsregeln in den Anschlussbedingungen zu verankern ist (ADR-1145), ohne dass die Infrastruktur die fachspezifischen Fristen selbst bestimmt (ADR-0001).

cc) Stellvertretung

Der Begriff der Stellvertretung erfasst in der Zielarchitektur zwei zu trennende Konstellationen: die organisationsinterne Bearbeitungsvertretung innerhalb der Bearbeitergruppen eines Funktionspostfachs (ADR-1102) und die externe Bevollmächtigung sowie die gesetzliche Vertretung, bei der eine Person im Namen einer anderen gegenüber der Verwaltung handelt (ADR-1113). Beide werfen unterschiedliche datenschutzrechtliche Fragen auf.

[279] Vgl. Moos/Rothkegel, in: Moos, Datenschutz und Datennutzung, 4. Aufl. 2024, M 12, Rn. 34 f.
[280] Moos/Rothkegel, aaO.

(1) Bearbeitungsvertretung innerhalb der Organisation

Die Bearbeitungsvertretung betrifft die Vertretung von Mitarbeitenden innerhalb der Bearbeitergruppe eines Funktionspostfachs. Sie wird umgesetzt, indem der Raum-Management-Service auf Grundlage des Berechtigungsverzeichnisses weitere berechtigte Personen in den bestehenden Vorgangsraum einlädt und ihnen – sofern ein E2EE-teilnehmender technischer Nutzer die Session-Schlüssel weitergibt – auch die bisherige Kommunikationshistorie zugänglich macht (ADR-1102, ADR-1112). Datenschutzrechtlich ist dieser Zugriff unproblematisch, solange er im administrativen Machtbereich der Organisation verbleibt: Die hinzutretende vertretende Person und der technische Nutzer sind keine Dritten im Sinne des Art. 4 Nr. 10 DSGVO, sondern unter der Verantwortung der Organisation befugte Stellen. Wird der technische Nutzer durch einen IT-Dienstleister betrieben, handelt dieser als Auftragsverarbeiter (Art. 28 DSGVO). Eine wirksame Ende-zu-Ende-Verschlüsselung schließt zwar den Zugriff der Infrastruktur und sonstiger Dritter aus,[281] nicht aber den Zugriff der befugten Bearbeitenden derselben verantwortlichen Stelle.

Die eigentliche datenschutzrechtliche Anforderung liegt damit nicht im Ausschluss dieses Zugriffs, sondern in seiner Begrenzung nach dem Need-to-know-Prinzip. Zugriff darf nur erhalten, wer ihn zur Aufgabenerfüllung benötigt. Die Berechtigungen sind durch ein dokumentiertes Berechtigungskonzept und, soweit erforderlich, durch menschliche Prüfung zu steuern.[282] Diese Anforderung verschärft sich in den bereichsspezifischen Geheimnisregimen: Das Sozialgeheimnis verpflichtet ausdrücklich, auch innerhalb des Leistungsträgers sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind (§ 35 Abs. 1 Satz 2 SGB I); entsprechendes kann sich ggf. – was durch die verantwortliche Stelle im Einzelnen zu prüfen ist – aus anderen Geheimnissen ergeben wie aus dem Steuergeheimnis oder berufsrechtlichen Verschwiegenheitspflichten. Die Zielarchitektur wird dem strukturell gerecht, indem jeder Vorgang in einem eigenen, kryptografisch isolierten Raum bearbeitet wird, dessen Mitgliederkreis über das Berechtigungsverzeichnis gesteuert und dessen Änderungen revisionssicher protokolliert werden (ADR-1102,

[281] Klein, in: Moos, Datenschutz und Datennutzung, 4. Aufl. 2024, M 28, Rn. 27.
[282] Vgl. Kramer/Meints, in: Auernhammer, DSGVO/BDSG, 8. Aufl. 2024, § 71 BDSG, Rn. 15; Thalhofer, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2025, § 16, Rn. 91.

ADR-1112). Die berechtigungsgesteuerte Isolierung verwirklicht die Zugänglichkeitsbegrenzung des Art. 25 Abs. 2 DSGVO und das Need-to-know-Prinzip zugleich. Für Bearbeitung mit besonders hohem Vertraulichkeitsbedarf hält die Architektur ferner die Konfiguration ohne E2EE-Teilnahme des technischen Nutzers bzw. die manuelle Raumverwaltung durch Moderatoren bereit (ADR-1102). In diesen Fällen ist eine automatisierte Vertretung nur eingeschränkt möglich, was der bewussten Priorisierung der Vertraulichkeit entspricht.

(2) Externe Bevollmächtigung und gesetzliche Vertretung

Für das Handeln im Namen einer anderen Person – etwa der steuerlichen Beratung aufgrund Vollmacht, der Prokura oder der gesetzlichen Vertretung durch Betreuende und Vormünder – stellte sich die Grundsatzfrage, ob die vertretende Person mit eigener Identität und eigenem Postfach auftritt oder auf das Postfach der vertretenen Person zugreift (ADR-1113). Die Zielarchitektur wählt zutreffend die erste Variante: Die vertretende Person nutzt ihre eigene (Berufs-)Identität und übermittelt den Nachweis der Vollmacht oder Vertretungsbefugnis entweder als Ergänzung des Identitätsnachweises (ADR-1106) oder als separates, gegebenenfalls signiertes Dokument (ADR-0017).

Diese Lösung ist datenschutzrechtlich dem Zugriff auf das fremde Postfach vorzuziehen. Sie wahrt die strikte Ende-zu-Ende-Verschlüsselung, weil kein fremder Klartextzugriff und keine geteilten Schlüssel erforderlich sind, und vermeidet die mit einem Fremdzugriff verbundenen Datenschutz- und Geheimnisschutzprobleme. Ein direkter Zugriff Dritter auf das Postfach einer anderen Person wird auch außerhalb dieses Kontexts nur als eng begrenzte Kompromisslösung für Ausnahmefälle für vertretbar gehalten.[283] Hinzu kommt, dass ein Fremdzugriff im Anwendungsbereich des Fernmeldegeheimnisses gesonderter Legitimation bedürfte: Die Wahrnehmung der Rechte am Telekommunikationsvorgang durch Bevollmächtigte oder rechtliche Betreuende ist nur nach Maßgabe der jeweiligen Vollmacht bzw. des betreuungsgerichtlich angeordneten Aufgabenkreises (vgl. §§ 1814, 1815 Abs. 2 Nr. 5 BGB) zulässig.[284] Indem die Zielarchitektur auf einen solchen Fremdzugriff verzichtet und stattdessen auf einen mit der Nachricht

[283] Rücker, in: Moos, Datenschutz und Datennutzung, 4. Aufl. 2024, M 24, Rn. 86.
[284] Heun, in: Auernhammer, DSGVO/BDSG, 8. Aufl. 2024, § 4 TDDDG, Rn. 7 f.

übermittelten Vertretungsnachweis setzt, umgeht sie diese Schwierigkeiten und bleibt zugleich frei von domänenspezifischer Logik (ADR-0001).

Konsequent ist auch die Entscheidung, die für Vollmachten und gesetzliche Vertretungen erforderlichen Register (Vollmachtsdatenbanken, Handelsregister, das derzeit fehlende Vormundschaftsregister) nicht selbst zu entwerfen. Ihre Führung und die Prüfung der Nachweise obliegen den zuständigen Stellen und Fachverfahren. Die Zielarchitektur ermöglicht lediglich die Übermittlung und Anzeige der Nachweise. Perspektivisch ist die Anbindung digitaler Vollmachten über die EUDI-Wallet bzw. die European Business Wallet vorgesehen (Digitalisierungsrichtlinie (EU) 2025/25, Vorschlag COM(2025)838). Dies berührt die datenschutzrechtliche Grundentscheidung nicht, sondern erweitert lediglich die Nachweisformate. Für die Praxis bleibt festzuhalten, dass die Beweislast und die Prüfung der Vertretungsmacht bei der empfangenden Stelle liegen und die Akzeptanz der Architektur insoweit von der Verfügbarkeit belastbarer Register abhängt (ADR-1113).

dd) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Grundentscheidung, keinen zentralen Aufbewahrungsdienst bereitzustellen und die Archivierung im Machtbereich der verantwortlichen Stelle zu belassen (ADR-1135), ist aus Sicht der Vereinbarkeit von Archivierung und Ende-zu-Ende-Verschlüsselung folgerichtig und beizubehalten. Die Übernahme über einen als E2EE-Teilnehmer konfigurierten technischen Nutzer bzw. das Endgerät samt standardisiertem Exportpaket ist die sachgerechte Umsetzung.

- Archivierung und Bearbeitungsvertretung setzen einen Entschlüsselungsendpunkt im administrativen Machtbereich der empfangenden Stelle voraus. Solange dieser gewahrt bleibt, liegt keine Offenlegung an Dritte vor (Art. 4 Nr. 9 und 10 DSGVO). Der Betrieb durch Dienstleister ist als Auftragsverarbeitung auszugestalten (Art. 28 DSGVO).

- Die kryptografische Isolierung je Vorgang und die berechtigungsgesteuerte Zugänglichkeit (ADR-1102, ADR-1112) verwirklichen Art. 25 Abs. 2 DSGVO und das Need-to-know-Prinzip. Sie sind angesichts der bereichsspezifischen Geheimnisregime (Sozialgeheimnis, Steuergeheimnis, Berufsgeheimnisse) konsequent umzusetzen und revisionssicher zu protokollieren.

- Für Kommunikation mit besonders hohem Schutzbedarf ist die nutzerzentrische Variante ohne serverseitigen Entschlüsselungsendpunkt (ADR-1101 Option A, ADR-1102) beizubehalten; der damit verbundene Verzicht auf automatisierte Vertretung und Historienzugriff ist als bewusste Priorisierung der Vertraulichkeit hinzunehmen.

- Für die externe Bevollmächtigung und die gesetzliche Vertretung ist die Lösung mit eigener Identität und übermitteltem Vertretungsnachweis (ADR-1113) datenschutzrechtlich vorzugswürdig. Ein Zugriff auf das Postfach der vertretenen Person ist zu vermeiden. Die Prüfung der Vertretungsmacht verbleibt bei den zuständigen Stellen. Die zugehörigen Register sind nicht Bestandteil der Infrastruktur (ADR-0001).

- Differenzierte Aufbewahrungs-, Zugriffs- und Löschregeln sind konfigurierbar zu halten und über die Anschlussbedingungen (ADR-1145) verbindlich zu machen; es verbleibt bei der datenschutzrechtlichen Verantwortung der jeweiligen Stelle. Für die zeitliche Dimension (Speicherbegrenzung, Archivrecht) wird auf Ziffer 3.5.1 verwiesen.

e) Schlüsselmanagement/-wiederherstellung und Auswirkungen auf Zugang und Zustellung

Kurzzusammenfassung. Das Schlüsselmanagement ist integraler Bestandteil der risikobasierten Sicherheitspflichten: Art. 32 DSGVO und Art. 25 DSGVO verlangen ein am Stand der Technik ausgerichtetes, dokumentiertes und auditierbares Verfahren für Erzeugung, Verteilung, Aufbewahrung, Rotation, Sperrung und Wiederherstellung der Schlüssel. Ergänzend greifen – bei Einordnung als digitaler Dienst bzw. Telekommunikationsdienst – § 19 TDDDG und das IT-Sicherheitsrecht. Darüber hinaus ist das Schlüsselmanagement für ZaPuK essentiell zur Begründung der Nicht-Anwendbarkeit des Datenschutzrechts auf der Inhaltsebene – dem Chiffrat

fehlt der Personenbezug aus Sicht der Betreiber nur, solange diese die Schlüssel nicht erlangen können (siehe 1.3).

Schließlich entscheidet das Schlüsselmanagement über die tatsächliche Verfügbarkeit der Nachricht für den Empfänger und damit über den wirksamen Zugang. Dabei ist die Ende-zu-Ende-Verschlüsselung mit den rechtlichen Zugangs- und Zustellmechanismen grundsätzlich vereinbar, weil sich die Nachweise über das verschlüsselte Chiffrat führen lassen (ADR-0017, ADR-0018) und der Ablauf einem „Sign-then-Encrypt" folgt. Ein wirksamer Zugang setzt aber die tatsächliche Möglichkeit der Kenntnisnahme voraus. Ein dauerhaft nicht entschlüsselbares Chiffrat gelangt nicht in wahrnehmbarer Form in den Machtbereich des Empfängers. Geht das Schlüsselmaterial ohne Wiederherstellungsmöglichkeit verloren, kann der Empfänger deshalb trotz vorliegender Bereitstellungsbestätigung den mangelnden Zugang geltend machen (§ 41 Abs. 2 Satz 3 VwVfG; ADR-0018, Risiko „Entschlüsselbarkeit"). Eine funktionierende, zugleich betreiberblinde Schlüsselwiederherstellung ist damit nicht nur eine Verfügbarkeits-, sondern eine Rechtssicherheitsanforderung mit Blick auf Bekanntgabe- und Zugangsfiktionen. Die Zielarchitektur trägt dem mit einem clientseitig verschlüsselten serverseitigen Schlüssel-Backup und einer Re-Authentisierungslösung im Grundsatz zutreffend Rechnung (Architekturkonzept, Abschnitt 5.4.13; ADR-1100). Die dedizierte Architekturentscheidung sollte in den PKI-Anforderungen und Anschlussbedingungen verankert werden (ADR-1144, ADR-1145).

aa) Schlüsselmanagement als Bestandteil der Sicherheitspflichten

Das Schlüsselmanagement ist wesentlicher Bestandteil des Einsatzes von Verschlüsselung. Die Wirksamkeit jeder kryptografischen Maßnahme steht und fällt mit der sicheren Erzeugung, Verteilung, Aufbewahrung und dem geordneten Lebenszyklus der Schlüssel. Rechtlich ist dies Teil der nach Art. 32 Abs. 1 DSGVO geschuldeten geeigneten technischen und organisatorischen Maßnahmen. Der dort geforderte Maßstab – Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie das Risiko für die Rechte und Freiheiten natürlicher Personen – ist an dem für ZaPuK festgestellten hohen Schutzbedarf auszurichten (Art. 32 Abs. 1 DSGVO). Hinzu tritt Art. 25 DSGVO, der verlangt, die Schlüsselarchitektur bereits bei der Festlegung der Mittel datenschutzfreundlich auszulegen; bei klassischer

Ende-zu-Ende-Verschlüsselung bedeutet dies, dass Schlüsselerzeugung und -haltung grundsätzlich clientseitig erfolgen und die Betreiberinfrastruktur nicht in den Besitz der Inhaltsschlüssel gelangt (Art. 25 Abs. 1 DSGVO; ADR-1100).

Der Stand der Technik ist eine dynamische Bezugsgröße, die sich fortlaufend an der technischen Entwicklung ausrichtet.[285] Als Orientierung dienen die einschlägigen Vorgaben des BSI, namentlich die Technische Richtlinie BSI TR-02102-1 zu kryptografischen Verfahren und Schlüssellängen sowie der Baustein CON.1 (Kryptokonzept) des IT-Grundschutz-Kompendiums. Danach kann ein unzureichendes oder fehlendes Schlüsselmanagement auch die Verfügbarkeit der Anwendungen bedrohen – ein Befund, der für die unten erörterte Zugangsfrage von unmittelbarer Bedeutung ist.[286] Ergänzend ist zu beachten, dass die eingesetzten Verfahren robust gegen künftige Angriffe sein müssen. Hierzu zählen ausreichende Schlüssellängen, das Prinzip der Perfect Forward Secrecy durch wechselnde Sitzungsschlüssel sowie die absehbare Migration hin zu quantensicheren Verfahren nach Maßgabe der jeweils aktuellen BSI-Empfehlungen.[287]

Wird ein ZaPuK-Postfach als digitaler Dienst bzw. – nach der telekommunikationsrechtlichen Einordnung (siehe V) – als interpersoneller Telekommunikationsdienst betrieben, treten spezialgesetzliche Sicherungsvorgaben hinzu. § 19 Abs. 4 TDDDG verlangt technische und organisatorische Vorkehrungen nach dem Stand der Technik gegen unerlaubten Zugriff und Störungen und nennt als Vorkehrung ausdrücklich die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens (§ 19 Abs. 4 Satz 3 TDDDG). § 19 Abs. 1 Nr. 2 und Abs. 2 TDDDG verpflichten überdies auf einen gegen Kenntnisnahme Dritter geschützten, nach Möglichkeit anonymen oder pseudonymen Dienst. Aus dem IT-Sicherheitsrecht folgt eine parallele Wertung. Das mit der NIS-2-Umsetzung neu gefasste BSIG zählt Konzepte und Prozesse für den Einsatz kryptografischer Verfahren ausdrücklich zu den Mindestmaßnahmen (§ 30 Abs. 2 Nr. 8 BSIG). Für die datenschutzrechtliche Beurteilung bestätigen diese Regime, dass ein geordnetes

[285] Vgl. Kramer/Meints, in: Auernhammer, 8. Aufl. 2024, Art. 32 DSGVO, Rn. 63.
[286] BSI, IT-Grundschutz-Kompendium, Baustein CON.1 Kryptokonzept.
[287] BSI TR-02102-1; Freund, in: Schuster/Grützmacher, IT-Recht, 2. Aufl. 2025, Art. 32 DSGVO, Rz. 45.

Kryptokonzept zum geschuldeten Standard gehört. Die bereichsspezifische Vertiefung erfolgt im IT-sicherheitsrechtlichen und im telekommunikationsrechtlichen Teil (siehe 2 und 3).

Aus dem Vorstehenden lassen sich die rechtlichen Kernanforderungen an das Schlüsselmanagement zusammenfassen. Erforderlich sind ein dokumentiertes, ISMS-gesteuertes Kryptokonzept mit klaren Rollen- und Rechtevorgaben; eine sichere, entropiestarke Schlüsselerzeugung mit geeigneten Parametern und der Trennung der Schlüsselräume nach Zweck (Inhalte, Metadaten-Signaturen, Transport – vgl. bereits ADR-1144); der Schutz privater Schlüssel gegen Export und Extraktion, im behördlichen Umfeld regelmäßig hardwaregestützt (Art. 32 DSGVO; ADR-1144); die Provider-Blindheit, also der grundsätzliche Verzicht auf eine serverseitige Haltung der Inhaltsschlüssel beim Betreiber; ein geordneter Lebenszyklus mit Rotation, Sperrung und Krypto-Agilität für die planvolle Migration bei kryptografischer Veralterung (ADR-0012, ADR-1144); sowie die Zugriffstrennung nach dem Prinzip der geringsten Rechte, gegebenenfalls mit Mehr-Augen- bzw. M-von-N-Freigaben für besonders sensible Schlüssel. Die Wirksamkeit dieser Maßnahmen ist nach Art. 32 Abs. 1 lit. d DSGVO regelmäßig zu überprüfen (zur Rechenschaftspflicht siehe D.III.4.).

bb) Doppelfunktion des Schlüsselmanagements: Vertraulichkeit und Verfügbarkeit

Für ZaPuK ist das Schlüsselmanagement in zweifacher Hinsicht ausschlaggebend, und zwar in einem Spannungsverhältnis, das nur durch eine sorgfältige Ausgestaltung aufgelöst werden kann.

Auf der einen Seite trägt die Ende-zu-Ende-Verschlüsselung ihre die Anwendbarkeit des Datenschutzrechts begrenzende Wirkung nur, solange die Betreiber die Schlüssel lückenlos nicht erlangen können (siehe 1.3). Der fehlende Personenbezug der Chiffrate beruht nicht auf einer endgültigen Beseitigung des Personenbezugs, sondern allein darauf, dass dem konkreten Akteur die Reidentifizierung nicht mit nach allgemeinem Ermessen wahrscheinlichen Mitteln möglich ist. Sobald ein Betreiber über einen Weg verfügt, den Schlüssel mit vertretbarem Aufwand zu erlangen – etwa über ein unzureichend gegen Betreiberzugriff abgesichertes serverseitiges Schlüssel-Backup –, wird das Chiffrat für ihn zu personenbezogenen Daten, und die datenschutzrechtlichen Pflichten leben insoweit auf. Die Ausgestaltung einer etwaigen

serverseitigen Schlüsselverwahrung ist damit nicht nur ein Sicherheits-, sondern zugleich ein anwendbarkeitsrelevanter Gestaltungsparameter. Das für ZaPuK vorgesehene Verfahren, das Schlüsselmaterial vor der Ablage auf dem Homeserver clientseitig zu verschlüsseln (Secure Secret Storage and Sharing), ist deshalb die datenschutzrechtlich gebotene Lösung: Es ermöglicht ein Backup, ohne dem Betreiber den Klartextzugriff auf die Schlüssel zu eröffnen (Architekturkonzept, Abschnitt 5.4.4 und 5.4.13; ADR-1100).

Auf der anderen Seite ist die Verfügbarkeit der Daten selbst ein datenschutzrechtliches Schutzziel. Nach Art. 32 Abs. 1 lit. b DSGVO ist die Verfügbarkeit auf Dauer sicherzustellen, und Art. 32 Abs. 1 lit. c DSGVO verlangt ergänzend die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Diese Wiederherstellbarkeit ist keine bloße Betriebsfrage, sondern eine ausdrücklich benannte Mindestmaßnahme, die erprobte Backup- und Recovery-Verfahren voraussetzt (Art. 32 Abs. 1 lit. c DSGVO).[288] Für ein verschlüsseltes System bedeutet dies, dass der Verlust des Schlüsselmaterials – etwa bei Verlust oder Defekt des Endgeräts – als ein solcher Zwischenfall zu behandeln ist, gegen den Vorsorge zu treffen ist. Ein Verzicht auf jede Wiederherstellungsmöglichkeit wäre daher nicht nur praktisch misslich, sondern mit dem Verfügbarkeitsgrundsatz nicht ohne Weiteres vereinbar.

Das eigentliche Problem liegt im Ausgleich beider Anforderungen: Ein Wiederherstellungsverfahren darf die Vertraulichkeit nicht dadurch preisgeben, dass es dem Betreiber Zugriff auf die Schlüssel verschafft. Verfügbarkeit und Zero-Access sind mithin gemeinsam zu verwirklichen. Die Zielarchitektur löst dies über zwei einander ergänzende Wege (Architekturkonzept, Abschnitt 5.4.13). Beim serverseitigen Schlüssel-Backup werden die Schlüssel clientseitig verschlüsselt und erst danach auf dem Homeserver hinterlegt. Die Wiederherstellung erfolgt durch einen ausschließlich beim Nutzer verwahrten Wiederherstellungsschlüssel, etwa in einem gesicherten Speicher des Geräts oder in einem ausdruckbaren Wiederherstellungsdokument. Bei der Wiederherstellung durch erneute Authentisierung kann eine Privatperson eine Kopie der verlorenen kanalbezogenen Schlüssel nach erfolgreicher Authentisierung auf hohem

[288] Kramer/Meints, in: Auernhammer, 8. Aufl. 2024, Art. 32 DSGVO, Rn. 45; Freund, in: Schuster/Grützmacher, IT-Recht, Art. 32 DSGVO, Rz. 102.

Vertrauensniveau erneut bei der jeweiligen Organisation anfordern. Beide Verfahren wahren die Betreiberblindheit und erfüllen zugleich die Verfügbarkeits- und Wiederherstellungsanforderung des Art. 32 DSGVO (Architekturkonzept, Abschnitt 5.4.13).

cc) Auswirkungen der Ende-zu-Ende-Verschlüsselung auf Zugang und Bekanntgabe

Die Ende-zu-Ende-Verschlüsselung ist mit den rechtlichen Mechanismen des Zugangs, der Bekanntgabe und der Zustellung im Ausgangspunkt vollständig vereinbar. Die für den Nachweis erforderlichen Vorgänge lassen sich über das verschlüsselte Chiffrat abbilden, ohne dass eine Inhaltskenntnis der Infrastruktur nötig wäre: Die Integrität und Herkunft des Dokuments werden vor dem Versand durch ein qualifiziertes Siegel bzw. eine qualifizierte Signatur gesichert (ADR-0017) und der Zugang der Nachricht (bzw. im Falle einer Zugangsfiktion die Bereitstellung) wird durch die serverseitig erzeugte, an den Ciphertext gebundene Bereitstellungsbestätigung belegt (ADR-0018). Dieser Ablauf entspricht dem Muster „Sign-then-Encrypt“, auf dem auch die etablierten Zustelldienste aufsetzen. Dass die Ende-zu-Ende-Verschlüsselung mit rechtsverbindlicher Übermittlung nicht in Widerspruch steht, zeigt sich zudem daran, dass der Gesetzgeber die verschlüsselte behördliche Kommunikation in konkreten Zusammenhängen bereits voraussetzt. So ermächtigt beispielsweise § 17 Abs. 1 Satz 2 Brennstoffemissionshandelsgesetz die zuständige Behörde, für die Kommunikation eine bestimmte Verschlüsselung vorzuschreiben.

Grenzen ergeben sich nicht aus der Verschlüsselung als solcher, sondern aus dem Zugangsbegriff (siehe II.2.1.1). Ein elektronisches Dokument geht erst zu, wenn es so in den Machtbereich des Empfängers gelangt ist, dass dieser unter gewöhnlichen Umständen die Möglichkeit der Kenntnisnahme hat (im Steuerverfahren muss das Dokument „in für den Empfänger bearbeitbarer Weise“ von der Empfangseinrichtung aufgezeichnet werden, § 87a Abs. 1 Satz 3 AO). Ein dauerhaft verschlüsseltes, mangels Schlüssel nicht lesbares Chiffrat erfüllt diese Voraussetzung nicht. Damit wirkt sich ein Schlüsselverlust unmittelbar auf die Wirksamkeit der Bekanntgabe aus: Die serverseitige Bereitstellungsbestätigung belegt den Eingang des Chiffrats im Postfach des Empfängers, nicht aber die Entschlüsselbarkeit der Nachricht (ADR-0018). Fehlt eine Wiederherstellungsmöglichkeit, kann der Empfänger deshalb trotz vorliegender

Bereitstellungsbestätigung geltend machen, die Nachricht sei ihm nicht in wahrnehmbarer Form zugegangen. Bei der elektronischen Übermittlung greift zu seinen Gunsten die Zweifelsregelung des § 41 Abs. 2 Satz 3 VwVfG (parallel § 37 Abs. 2 Satz 3 SGB X, § 122 Abs. 2a AO), wonach im Zweifel die Behörde den Zugang nachzuweisen hat. Bei den für ZaPuK zentralen Abruf- und Bereitstellungsmodellen (§ 9 OZG, § 41 Abs. 2a VwVfG, § 122a AO) kann der Empfänger überdies einwenden, dass die gesetzlich geforderte Speicher- und Abrufbarkeit gerade nicht gewährleistet war, weil das bereitgestellte Dokument nicht in lesbarer Form gespeichert werden konnte (§ 9 Abs. 1 Satz 3 OZG; § 41 Abs. 2a Satz 2 VwVfG).

Für die Beurteilung der Zugangs- und Bekanntgabefiktionen folgt daraus eine wichtige Präzisierung. Die Fiktionen der § 9 Abs. 1 Satz 4 OZG und § 122a Abs. 4 AO knüpfen die Bekanntgabe an die Bereitstellung zum Abruf und verlangen zugleich, dass die Behörde die Speicherbarkeit gewährleistet. Setzt die tatsächliche Wahrnehmbarkeit der bereitgestellten Nachricht aber die Entschlüsselbarkeit voraus, so ist eine funktionierende Schlüsselwiederherstellung die Bedingung dafür, dass die Fiktion überhaupt eingreifen kann. Anderenfalls würde die Fiktion an einen bloß formalen Bereitstellungsvorgang anknüpfen ohne Rücksicht auf die Nutzbarkeit (Entschlüsselbarkeit, Lesbarkeit) des Empfangenen für den Empfänger. Eine solche gesetzliche Fiktion dürfte mit den Garantien des Grundgesetzes unvereinbar sein. Sie würde Widerspruchs- und Rechtsmittelfristen in Gang setzen, obwohl der Betroffene vom Inhalt des Verwaltungsakts keine Kenntnis nehmen kann. Eine solche Regelung liefe Gefahr, die Rechtsschutzgarantie (Art. 19 Abs. 4 GG), den Anspruch auf rechtliches Gehör (Art. 103 Abs. 1 GG), das Rechtsstaatsprinzip und den allgemeinen Justizgewährungsanspruch zu verletzen (Art. 20 Abs. 3 GG iVm Art. 2 Abs. 1 GG). Auf unionsrechtlicher Ebene läge ein Verstoß gegen Art. 47 EU-Grundrechtcharta nahe. Der EuGH verlangt für den wirksamen gerichtlichen Rechtsschutz nicht nur einen tatsächlichen Zugang der Entscheidung, sondern eine Zustellung, die es dem Adressaten erlaubt, genaue Kenntnis von den Gründen und den Rechtsbehelfen samt Frist zu nehmen, um seine Rechte wirksam wahrnehmen zu können.[289]

[289] EuGH, Urteil vom 04.11.2021 – C-338/20, Rn. 34.

Die Schlüsselwiederherstellung ist damit nicht allein eine Frage der Datenverfügbarkeit, sondern eine Voraussetzung der Rechtssicherheit des fingierten Zugangs. Dieser Zusammenhang ist auch in der Zielarchitektur ausdrücklich benannt (ADR-0018, Risiko „Entschlüsselbarkeit"; Architekturkonzept, Abschnitt 5.4.13) und bestätigt, dass die Schlüsselverwaltung mit Wiederherstellungsmöglichkeit in der Zielarchitektur zwingend umzusetzen ist.

dd) Nicht entschlüsselbare Nachrichten als Fehlerfall

Die allgemeinen Rechtsfolgen unzustellbarer oder fehlerhaft verschlüsselter Nachrichten – differenziert nach Bekanntgabemodell und Beweislastverteilung – sind gesondert dargestellt (siehe VII.1). Aus der hier maßgeblichen Perspektive des Schlüsselmanagements ist der Schlüsselverlust lediglich eine besonders praxisrelevante Fehlerursache innerhalb dieses Spektrums, das auch Client-Fehler, defekte Token und systemseitige Fehler in der Ver- und Entschlüsselungskette umfasst. Für sämtliche dieser Konstellationen gilt der bereits entwickelte Grundsatz: Ein Fehler, der die Lesbarkeit beim Empfänger dauerhaft verhindert, steht dem wirksamen Zugang entgegen, und seine praktische Durchschlagskraft hängt von der Beweislastverteilung unter dem jeweiligen Modell ab.

Bedeutsam ist, dass das geltende Recht bereits einen Reparaturmechanismus vorsieht, der die Folgen einer fehlenden Entschlüsselbarkeit abmildert. Macht der Empfänger geltend, er könne das übermittelte Dokument nicht bearbeiten, hat die Behörde es ihm erneut in einem geeigneten Format oder als Schriftstück zu übermitteln (§ 3a Abs. 4 Satz 2 VwVfG; parallel § 87a Abs. 2 Satz 2 AO). Für ZaPuK bedeutet dies, dass ein erkannter Entschlüsselungsfehler nicht zwingend zum endgültigen Scheitern der Bekanntgabe führt, sofern die Infrastruktur den Fehler erkennt und eine erneute, entschlüsselbare Bereitstellung ermöglicht. Die vertraulichkeitswahrende Schlüsselwiederherstellung ergänzt diesen Mechanismus, indem sie den Regelfall des Schlüsselverlusts auflöst, bevor es zu einem Zugangsstreit kommt. Zu berücksichtigen ist, dass das Verwaltungsverfahrensrecht durch das Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern neu geordnet wird; die Neufassung der §§ 3a bis 3c VwVfG tritt allerdings erst zum 1. Juli 2027 in Kraft, sodass bis dahin der bestehende § 3a Abs. 4 VwVfG

maßgeblich bleibt.[290] Die einschlägigen Zugangs- und Fiktionsregelungen der § 41 VwVfG, § 9 OZG, § 122a AO und § 37 SGB X bleiben von der Reform unberührt.

ee) Übertragung auf ZaPuK

Die Zielarchitektur bildet die vorstehenden Anforderungen im Grundsatz zutreffend ab. Die Ende-zu-Ende-Verschlüsselung terminiert für die Einzelnutzer-Kommunikation ausschließlich im Endgerät (ADR-1100), das private Schlüsselmaterial verlässt das Gerät nicht, und die kryptografischen Operationen werden im zentral bereitgestellten SDK gekapselt, was zugleich die geforderte Krypto-Agilität und einen späteren Wechsel des Verschlüsselungsprotokolls (etwa hin zu MLS) erleichtert (ADR-0012; Architekturkonzept, Abschnitt 5.4.4). Für die Schlüsselwiederherstellung sieht die Architektur mit dem clientseitig verschlüsselten serverseitigen Schlüssel-Backup und der Re-Authentisierung zwei betreiberblinde Verfahren vor, die Verfügbarkeit und Vertraulichkeit gleichermaßen wahren (Architekturkonzept, Abschnitt 5.4.13; ADR-1100). Diese Ausgestaltung ist datenschutzrechtlich tragfähig.

Die Architekturentscheidung zur Schlüsselwiederherstellung (Architekturkonzept 5.4.13) hat Bedeutung für die Anwendbarkeit des Datenschutzrechts auf der Inhaltsebene sowie für die Rechtssicherheit der Zugangs- und Bekanntgabefiktionen. Dabei ist insbesondere sicherzustellen, dass ein serverseitiges Schlüssel-Backup dem Betreiber unter keinen Umständen den Zugriff auf die Inhaltsschlüssel eröffnet, dass die Wiederherstellung dem berechtigten Nutzer zeitnah und ohne unzumutbare Hürden möglich ist und dass die Re-Authentisierung nur auf hohem Vertrauensniveau erfolgt (dies entspricht dem Architekturkonzept, Abschnitt 5.4.13).

ff) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Das Schlüsselmanagement ist als geschuldete Sicherheitsmaßnahme nach Art. 32 und Art. 25 DSGVO in einem dokumentierten, ISMS-gesteuerten Kryptokonzept am Stand der Technik (BSI TR-02102-1, IT-Grundschutz CON.1) auszurichten. Die

[290] Art. 1 Nr. 3, Art. 16 Abs. 4 des Gesetzes vom 3. Juli 2026, BGBl. 2026 I Nr. 199.

Grundentscheidungen zur clientseitigen Schlüsselhaltung und zur Krypto-Agilität (ADR-1100, ADR-1144) sind folgerichtig. Die Migrationsfähigkeit hin zu quantensicheren Verfahren ist vorzusehen.

- Der fehlende Personenbezug der Inhalte für die Betreiber steht und fällt mit der lückenlosen Unmöglichkeit des Schlüsselzugriffs. Ein serverseitiges Schlüssel-Backup ist daher zwingend so auszugestalten, dass die Schlüssel vor der Ablage clientseitig verschlüsselt werden und der Betreiber sie auch nicht mit vertretbarem Aufwand erlangen kann (dies entspricht dem Architekturkonzept, Abschnitt 5.4.13).

- Die Schlüsselwiederherstellung ist zugleich Verfügbarkeitspflicht (Art. 32 Abs. 1 lit. b und c DSGVO) und Voraussetzung der Rechtssicherheit des fingierten Zugangs (§ 9 OZG, § 122a AO, § 41 Abs. 2a VwVfG). Ein vollständiger Verzicht auf jede Wiederherstellung wäre aus rechtlicher Sicht mit dem Verfügbarkeitsgrundsatz sowie mit der angestrebten Tragfähigkeit der Bekanntgabefiktionen unvereinbar.

- Die Ende-zu-Ende-Verschlüsselung ist mit den rechtlichen Institutionen des Zugangs, der Bekanntgabe und der Zustellung vereinbar. Die Nachweise werden über das Chiffrat geführt (ADR-0017, ADR-0018). Die Bereitstellungsbestätigung belegt den Eingang, nicht die Entschlüsselbarkeit; auf diese Grenze ist im Nachweiskonzept Rücksicht zu nehmen.

- Für den Fehlerfall der Nichtentschlüsselbarkeit sollte die Infrastruktur einen Erkennungs- und Rückkanal vorsehen, der – im Einklang mit der Wertung des § 3a Abs. 4 Satz 2 VwVfG und des § 87a Abs. 2 Satz 2 AO – eine erneute, entschlüsselbare Bereitstellung anstößt, bevor eine Fiktion greift. Zu Rechtsfolgen technischer Zustellungsfehler siehe VII.1.

- Verbindliche Vorgaben zu Schlüsselerzeugung, betreiberblindem Backup, Wiederherstellung, Rotation und Sperrung sind über die Anschlussbedingungen (ADR-1145) zu transportieren, ohne die eigenständige datenschutzrechtliche Verantwortung der jeweiligen Stelle zu verlagern.

3.6.3. Vertraulichkeit der Kommunikationsbeziehung (Metadatenschutz)

Kurzzusammenfassung. Während die vorstehenden Abschnitte die Vertraulichkeit der Nachrichteninhalte behandeln, betrifft dieser Abschnitt die Vertraulichkeit der Kommunikationsbeziehung als solcher, also den Schutz der Kommunikationsmetadaten. Diese Metadaten fallen im Postfach-Backend nach dem Matrix-Protokoll zwangsläufig unverschlüsselt an und bleiben trotz pseudonymer Adressierung für die Betreiber personenbezogen. Die Ende-zu-Ende-Verschlüsselung wirkt sich auf sie gerade nicht aus (siehe 1.3). Ihr Schutzbedarf ist hoch und kann denjenigen der Inhalte erreichen oder übersteigen, weil schon aus dem Umstand, wer wann mit wem kommuniziert, hochsensible Informationen und bei massenhafter Korrelation Risiken bis hin zur nationalen Sicherheit folgen können.

Rechtlich wird der Metadatenschutz von mehreren Seiten getragen: von den Grundsätzen der Datenminimierung und der Zweckbindung sowie den Pflichten zu Datenschutz durch Technikgestaltung und zur Sicherheit der Verarbeitung (Art. 5, 25, 32 DSGVO), im JI-Bereich ergänzt um das Gebot frühestmöglicher Pseudonymisierung und die Kontrollmaßnahme der Trennbarkeit (§ 63, § 71 BDSG, Art. 29 JI-RL), und – soweit ein Postfach als Telekommunikationsdienst einzuordnen ist – vom Fernmeldegeheimnis, das ausdrücklich auch die Tatsache erfasst, ob jemand an einem Telekommunikationsvorgang beteiligt war (§ 3 TDDDG, Art. 10 GG). Der von der Zielarchitektur verfolgte Betreiberausschluss – die Verhinderung, dass ein einzelnes Rechtssubjekt die Metadaten der Bürger- und der Organisationsdomäne zusammenführen kann – ist damit kein bloßes Sicherheitsanliegen, sondern datenschutz- und ggf. telekommunikationsrechtlich geboten.

Die architektonischen Grundentscheidungen zur Metadatenreduktion, zur getrennten Betreiberstruktur und zur bereichsspezifischen pseudonymen Adressierung (ADR-1103, ADR-1104, ADR-1105) verwirklichen dieses Ziel. Ihre rechtliche Absicherung hängt vom Betriebsmodell ab: Werden die Backends durch verschiedene Rechtssubjekte betrieben, stützt bereits die organisatorische Trennung in Verbindung mit dem Datenschutz- und ggf. Telekommunikationsrecht den Ausschluss. Sie sollte durch ausdrückliche Zusammenführungs- und Querzugriffsverbote in Vergabe und Verträgen, durch Change-Control-Klauseln und perspektivisch durch eine

spezialgesetzliche Regelung verstärkt werden. Werden beide Bestände durch dasselbe Rechtssubjekt in Auftragsverarbeitung verantwortet, genügt eine bloße Pflicht zur Offenlegung unberechtigter Zusammenführungsweisungen nicht. Sie ist sinnvoll, aber nicht hinreichend, weil sich das Weisungsrecht des Verantwortlichen im Grundsatz durchsetzt und der Verantwortliche auch auf anderen Wegen als über eine Weisung Zugriff nehmen könnte. Erforderlich ist vielmehr, dass die Systeme so gebaut werden, dass domänenübergreifende Verknüpfung technisch ausgeschlossen ist, flankiert von einem gesetzlichen Zusammenführungsverbot und Change-Control-Vorbehalten.

a) Schutzgut und Schutzbedarf der Kommunikationsmetadaten

Gegenstand dieses Abschnitts ist nicht der Inhalt, sondern die Beziehung: wer mit welcher Stelle, zu welchem Zeitpunkt und in welcher Häufigkeit kommuniziert. Diese Metadaten fallen im Betrieb notwendig an – teils zwingend auf der Netzwerkebene (etwa IP-Adressen), teils als unverschlüsselte Adressierungs- und Routing-Informationen des Matrix-Protokolls – und können durch die betreibenden Stellen grundsätzlich eingesehen werden. Ihr Schutzbedarf ist erheblich. Bereits das Bekanntwerden einer Kommunikationsverbindung kann diskriminierungssensible Rückschlüsse ermöglichen, etwa die Kommunikation einer Privatperson mit einer bestimmten Facharztpraxis oder mit einer spezifischen Fachbehörde. Aus solchen Beziehungen lassen sich Lebenslagen rekonstruieren und Erpressbarkeiten begründen. Die Möglichkeit der massenhaften Korrelation lässt bei einer Kompromittierung zentraler Komponenten Schäden bis hin zu Risiken für die nationale Sicherheit entstehen. Diese Einschätzung liegt der Zielarchitektur zugrunde (Architekturkonzept, Abschnitt 5.4.11 Metadatenreduktion).

Der EuGH hat für Verkehrs- und Standortdaten wiederholt hervorgehoben, dass sie präzise Schlüsse auf das Privatleben zulassen und deshalb nicht weniger sensibel sind als Kommunikationsinhalte.[291] Das BVerfG ordnet die Kommunikationsumstände – insbesondere ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Telekommunikationsverkehr stattgefunden hat – ausdrücklich dem Schutzbereich des Art. 10 Abs. 1 GG zu und erstreckt diesen

[291] Vgl. EuGH, Urt. v. 30.04.2024 – C-470/21 – La Quadrature du Net u.a., ECLI:EU:C:2024:370 (zur ePrivacy-Richtlinie 2002/58/EG).

Schutz auf die an die Kenntnisnahme anschließenden Verarbeitungs- und Verwendungsvorgänge.[292] In besonders gelagerten Konstellationen tritt ein spezifisches Vertraulichkeitsinteresse hinzu, etwa beim Schutz von Informantinnen und Informanten, V-Personen und verdeckten Ermittlern, aber auch beim publizistischen Quellenschutz, den der Europäische Gerichtshof für Menschenrechte der Kommunikationsfreiheit zuordnet.[293] Die Vertraulichkeit der bloßen Kontaktaufnahme kann in diesen Fällen für Leib und Leben der Beteiligten von Bedeutung sein. Das Vertraulichkeitsgebot des § 8 Hinweisgeberschutzgesetz bildet insoweit eine flankierende, wenn auch nicht unmittelbar einschlägige gesetzgeberische Wertung.

b) Der rechtliche Rahmen des Metadatenschutzes

Datenschutzrechtlich bleiben die Kommunikationsmetadaten auch bei bereichsspezifischer pseudonymer Adressierung personenbezogen. Die Pseudonymisierung beseitigt den Personenbezug nicht, sondern ersetzt lediglich den unmittelbaren Identifikator. Für das Backend, das die pseudonyme Adresse den zugehörigen Vorgängen zuordnet und – im Antragskontext – aus der Identität ableitet, bleibt die betroffene Person mit nach allgemeinem Ermessen wahrscheinlichen Mitteln zumindest indirekt bestimmbar (siehe 1.3). Anders als auf der Inhaltsebene, die für die reinen Transport- und Speicherakteure mangels Schlüsselzugriffs anonym ist, unterfällt die Metadatenverarbeitung durch die Postfach-Backends daher der DSGVO. Maßgeblicher Bewertungsmaßstab sind der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) sowie – für die technische Gestaltung – Art. 25 DSGVO, der die Datenminimierung ausdrücklich auf die Zugänglichkeit der Daten erstreckt (Art. 25 Abs. 2 DSGVO), und Art. 32 DSGVO, der ein am hohen Risiko orientiertes Schutzniveau verlangt und Pseudonymisierung als geeignete Maßnahme benennt (Art. 32 Abs. 1 lit. a DSGVO). Das eigentliche Schutzziel lässt sich als Nichtverkettbarkeit beschreiben:

[292] BVerfG, Beschluss vom 08.10.2024 – 1 BvR 1743/16, 1 BvR 2539/16, Rn. 136 f., ECLI:DE:BVerfG:2024:rs20241008.1bvr174316; bereits BVerfG, Beschluss vom 13.11.2010 – 2 BvR 1124/10, Rn. 12, ECLI:DE:BVerfG:2010:rk20101113.2bvr112410.

[293] EGMR, Urteil vom 27.03.1996 – Nr. 17488/90 – Goodwin/Vereinigtes Königreich, Rn. 39; Art. 10 EMRK.

Daten, die zweckgebunden für die Übermittlung anfallen, dürfen nicht domänenübergreifend korreliert und zu Profilen zusammengeführt werden.

Im Anwendungsbereich der JI-Richtlinie – für ZaPuK relevant, soweit über das Justiz-Backend zu den Zwecken des § 45 BDSG verarbeitet wird – wird dieses Ziel verschärft. § 71 BDSG verpflichtet ausdrücklich zur Datensparsamkeit und zur frühestmöglichen Pseudonymisierung, und die Kontrollmaßnahmen des § 63 BDSG, die Art. 29 JI-RL umsetzen, nennen die Trennbarkeit als eigenständige technisch-organisatorische Anforderung.[294] Die getrennte Haltung von Datenbeständen ist damit im JI-Bereich nicht nur zulässig, sondern als Sicherungsmaßnahme vorgezeichnet. Ihre Wertung lässt sich für den übrigen, DSGVO-getragenen Teil der Infrastruktur als Konkretisierung dessen heranziehen, was Datenminimierung und Zweckbindung verlangen.

Soweit ein Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu V), tritt das Fernmeldegeheimnis als drittes, teils schärfstes Schutzregime hinzu. § 3 Abs. 1 TDDDG erstreckt das Fernmeldegeheimnis ausdrücklich auf die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, und damit gerade auf die hier interessierende Kommunikationsbeziehung. § 3 Abs. 3 TDDDG untersagt den Verpflichteten, sich über das für die Diensterbringung erforderliche Maß hinaus Kenntnis von den näheren Umständen der Kommunikation zu verschaffen, erlaubt eine Verwendung erlangter Kenntnisse nur für diesen Zweck und lässt eine Weitergabe an andere nur zu, soweit ein Gesetz dies ausdrücklich und mit Bezug auf Telekommunikationsvorgänge vorsieht. Diese Bindung wirkt kraft Gesetzes und steht nicht zur Disposition des Auftraggebers; für die weitere Beurteilung ist dies von zentraler Bedeutung. Ergänzend verlangt das Verkehrsdatenrecht die unverzügliche, zweckgebundene Löschung (§ 9 TDDDG), was das Anfallen korrelierbarer Bestände von vornherein begrenzt.

c) Der Betreiberausschluss als Umsetzung des Metadatenschutzes

Unter Betreiberausschluss versteht die Zielarchitektur den Schutz sensibler Metadaten vor dem Zugriff des Anbieters oder Betreibers der Infrastruktur durch organisatorische Trennung

[294] Dazu Kramer/Meints, in: Auernhammer, DSGVO/BDSG, 8. Aufl. 2024, § 63 BDSG, Rn. 9.

zwischen den Betreibern der Infrastruktur für Privatpersonen und für Organisationen, damit die beiderseitigen Bestände nicht zusammengeführt werden können und die Kontaktaufnahme vertraulich bleibt. Dieses Ziel ist nach dem Vorstehenden datenschutzrechtlich geboten und im Telekommunikationsrecht vorgezeichnet. Die Architektur setzt es auf mehreren Ebenen um: Der wirksamste Beitrag besteht darin, schützenswerte Metadaten möglichst gar nicht erst entstehen zu lassen, etwa durch das für die Privatpersonen-Domäne vorgesehene Protokollierungsverbot für IP-Adressen. Wo Metadaten unvermeidbar anfallen, verhindert die bereichsspezifische pseudonyme Adressierung eine bereichsübergreifende Verkettung über einen einheitlichen Identifikator (ADR-1105), und die getrennte Betreiberstruktur mit einem eigenen Backend je Teilnehmergruppe entzieht einem einzelnen Betreiber den gleichzeitigen Zugriff auf die Bestände beider Domänen (ADR-1103). Die Anschlussbedingungen sehen hierzu bereits eine nur zweckgebundene Auswertung betriebsbedingt anfallender Metadaten sowie ein ausdrückliches Zusammenführungs- und Querzugriffsverbot zwischen Bürger- und Organisationsdomäne vor (ADR-1145).

Eine Grenze der Domänentrennung ergibt sich dort, wo dieselbe natürliche Person in beiden Domänen auftritt. Freiberuflich oder gewerblich tätige Einzelpersonen können sowohl ein Bürgerkonto als auch ein Organisationskonto nutzen (§ 2 Abs. 5 Satz 3 und 4 OZG), und der zentrale Postfachzugang soll solche Doppelrollen ausdrücklich abbilden (Architekturkonzept, Abschnitt 5.4.2). Datenschutzrechtlich ist das unbedenklich, solange die Zusammenführung ausschließlich im Endgerät der betroffenen Person stattfindet und beide Bereiche im Backend über getrennte, nicht aufeinander abbildbare Adressen geführt werden. Auszuschließen sind demgegenüber eine serverseitige Verknüpfung der beiden Postfächer und eine Ableitung der Organisationsadresse aus dem Bereichspseudonym der Privatperson; beides hebelte den Betreiberausschluss gerade für diejenige Gruppe aus, bei der private und berufliche Kommunikation dieselbe Person betreffen. Der Gesetzgeber hat eine entsprechende Kontexttrennung für das Unternehmensbasisregister bereits angeordnet: Jede einzelne wirtschaftliche Tätigkeit wird dort als eigenes Unternehmen geführt, und Daten zu natürlichen Personen ohne Bezug zu einer wirtschaftlichen Tätigkeit werden nicht gespeichert (§ 3 Abs. 1 Satz 2 und 3 UBRegG). Diese

Wertung lässt sich auf die Zuordnung zu den Postfach-Backends übertragen: Maßgeblich ist nicht der Status der handelnden Person, sondern der Kontext der jeweiligen Kommunikation.

Nichts anderes gilt für die vorgesehene Registrierung von Berufsträgern im Adressregister (Architekturkonzept, Abschnitt 5.5.1.3). Sie steht nicht im Widerspruch dazu, dass Privatpersonen dort nicht verzeichnet werden (ADR-1111), weil sie die betreffenden Personen allein in ihrer beruflichen Sphäre erfasst. Deren Erreichbarkeit ist ohnehin öffentlich zugänglich: Die berufsständischen Gesamtverzeichnisse führen Namen, Anschrift und geschäftliche Telekommunikationsdaten und enthalten ausdrücklich auch die Bezeichnung des besonderen elektronischen Postfachs; die Einsicht steht jedermann unentgeltlich zu (§ 31 Abs. 2, 3 und 5 BRAO; § 86b Abs. 1 bis 3 StBerG). Vorausgesetzt ist auch hier, dass die Berufsadresse von der privaten Bereichsadresse derselben Person getrennt bleibt und nicht auf sie abbildbar ist. Die Zielarchitektur trägt dem Rechnung, indem Berufsträger für ihre berufliche Tätigkeit eigene Konten und Adressen verwenden.

Der Schutzwert der Trennung steht und fällt allerdings damit, dass kein Rechtssubjekt rechtlich und zugleich technisch in der Lage ist, die getrennten Bestände wieder zusammenzuführen. Die Wirksamkeit des Betreiberausschlusses ist deshalb eine Frage der gewählten Verantwortlichkeits- und Betriebskonstellation. Insoweit sind zwei Szenarien zu unterscheiden.

aa) Szenario A: Betrieb durch verschiedene Rechtssubjekte

Werden das Backend für Privatpersonen und dasjenige für Organisationen durch verschiedene Rechtssubjekte betrieben – etwa durch den Bund einerseits und eine vom IT-Planungsrat getragene Stelle andererseits –, ist der Betreiberausschluss bereits weitgehend gesichert. Jeder Betreiber ist für die bei ihm anfallenden Metadaten eigenständig datenschutzrechtlich verantwortlich und hat weder rechtlich noch tatsächlich Zugriff auf den Bestand des jeweils anderen. Eine domänenübergreifende Zusammenführung würde eine Übermittlung zwischen zwei getrennten Verantwortlichen voraussetzen, die einer eigenen Rechtsgrundlage bedürfte und an den Grundsätzen der Zweckbindung und Datenminimierung zu messen wäre; ohne eine solche Grundlage ist sie unzulässig. Soweit die Dienste als Telekommunikationsdienste einzuordnen sind, verstärkt das Fernmeldegeheimnis diese Trennung, weil § 3 Abs. 3 TDDDG die Weitergabe

an andere ohne ausdrückliche gesetzliche Grundlage verbietet. Diese Konstellation trägt zudem der architektonischen Erwägung Rechnung, dass die organisatorische Trennung der Betreiber gerade verhindern soll, dass eine Stelle zugleich Zugriff auf die Metadaten von Absender- und Empfängerseite erlangt (Architekturkonzept, Abschnitt 4.2.1).

Gleichwohl ist zu empfehlen, den Betreiberausschluss nicht allein der allgemeinen Rechtslage zu überlassen, sondern ausdrücklich abzusichern. In der Vergabe- und Vertragsgestaltung sollten Zusammenführungs- und Querzugriffsverbote für Metadaten verankert und bei Einschaltung von Subunternehmern durch Spiegelung der Klauseln durchgereicht werden. Diese vertraglichen Vorgaben sollten durch ein verbindliches technisches Regelwerk unterlegt und durch Change-Control-Klauseln geschützt werden, die eine spätere einseitige Änderung in Richtung einer Verknüpfung ausschließen oder an enge Voraussetzungen binden. Innerorganisatorisch empfiehlt es sich, den Betreiberausschluss als Prüf- und Steuerungsziel in das Informationssicherheits- und Datenschutzmanagement sowie in die Datenschutz-Folgenabschätzung aufzunehmen. Perspektivisch kommt – parallel zur Wertung des § 3 Abs. 3 TDDDG – ein ausdrückliches gesetzliches Verbot der Zusammenführung und Verknüpfung von Metadaten zwischen den Betreibern der Bürger- und der Organisationsdomäne in Betracht, das Rechtssicherheit schafft.

bb) Szenario B: Betrieb durch dasselbe Rechtssubjekt in Auftragsverarbeitung

Problematischer ist es, wenn beide Infrastrukturen einschließlich der jeweiligen Metadatenbestände in der datenschutzrechtlichen Verantwortlichkeit desselben Rechtssubjekts stehen und der getrennte Betrieb lediglich im Wege der Auftragsverarbeitung organisiert ist. Hier fehlt die trennende Wirkung getrennter Verantwortlichkeiten, weil der Verantwortliche über Zwecke und Mittel beider Verarbeitungen bestimmt und den Auftragsverarbeitern gegenüber weisungsbefugt ist. Der Betreiberausschluss muss dann gegen den Verantwortlichen selbst wirken.

Die im Ausgangspunkt naheliegende Überlegung, den Ausschluss über eine Pflicht der Auftragsverarbeiter zur Offenlegung einer unberechtigten Aufforderung zur Zusammenlegung der Datenbestände abzusichern, greift zu kurz. Zwar ist eine solche Offenlegungspflicht vertragsrechtlich voraussichtlich zulässig und wirksam und knüpft an die ohnehin bestehende

Benachrichtigungspflicht des Art. 28 Abs. 3 Unterabs. 2 DSGVO an, nach der der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren hat, wenn er eine Weisung für datenschutzwidrig hält.[295] Sie ist insofern sinnvoll, aber für sich genommen nicht hinreichend. Das folgt aus drei Erwägungen.

Erstens setzt sich die Weisungsbefugnis des Verantwortlichen im Grundsatz durch: Bestätigt er die Weisung und besteht auf ihrer Befolgung, ist der Auftragsverarbeiter regelmäßig zur Umsetzung verpflichtet; nur bei offensichtlichen Rechtsverstößen wird er von der Befolgungspflicht entbunden.[296] Eine Offenlegungspflicht erzeugt damit Transparenz gegenüber der Aufsicht, verhindert aber keine rechtmäßig neu erteilte oder geänderte Weisung. Zweitens ist die Benachrichtigung in Szenario B strukturell begrenzt, weil sie sich an den Verantwortlichen richtet – also gerade an diejenige Stelle, von der die Aufforderung zur Zusammenführung ausgeht. Eine vertragliche Pflicht zur Offenlegung gegenüber der Allgemeinheit ist zwar möglich, aber offensichtlich schwer durchsetzbar (selbst wenn sie als echter Vertrag zugunsten Dritter gestaltet wäre). Drittens erfasst die Betrachtung, die allein auf die Weisung zur Zusammenlegung abstellt, nicht sämtliche Gefährdungen der Metadatenvertraulichkeit. Der Verantwortliche könnte die Vertraulichkeit auch auf anderem Wege gefährden, etwa indem er in beide Bestände Einsicht nimmt und diese anschließend selbst querverknüpft. Das Setup muss deshalb nicht nur gegen die Weisung zur Zusammenlegung, sondern gegen den domänenübergreifenden Zugriff insgesamt schützen.

Aus diesem Befund folgt, dass der Betreiberausschluss in Szenario B primär technisch zu verwirklichen ist. Die Systeme sind so zu gestalten, dass der Verantwortliche keine technische Schnittstelle erhält, mit der er die Metadaten der beiden Domänen domänenübergreifend verknüpfen kann. Dies ist die konsequente Anwendung des Art. 25 DSGVO, der verlangt, die Datenschutzgrundsätze durch Technikgestaltung wirksam umzusetzen und die Zugänglichkeit der Daten durch Voreinstellung zu begrenzen (Art. 25 Abs. 1 und 2 DSGVO). Eine so verankerte technische Nichtverkettbarkeit wirkt unabhängig von der Weisungslage und ist deshalb dem bloß vertraglichen Schutz überlegen. Sie sollte durch Change-Control-Klauseln ergänzt

[295] Dazu Freund, in: Schuster/Grützmacher, IT-Recht, 2. Aufl. 2025, Art. 28 DSGVO, Rz. 122.
[296] Vgl. Freund, in: Schuster/Grützmacher, IT-Recht, 2. Aufl. 2025, Art. 28 DSGVO, Rz. 124.

werden, die eine Änderung der technischen und vertraglichen Vorgaben in Richtung einer Verknüpfung ausschließen oder nur unter engen Voraussetzungen zulassen, etwa bei einer Gesetzesänderung oder nach Genehmigung durch die Aufsichtsbehörde. Soweit die Dienste als Telekommunikationsdienste einzuordnen sind, tritt das Fernmeldegeheimnis als gesetzliche Schranke hinzu, die auch den im Auftrag tätigen Betreiber bindet und eine zweckwidrige Verwendung oder Weitergabe der Beteiligungsdaten unabhängig von einer Weisung des Auftraggebers untersagt (§ 3 Abs. 3 TDDDG). Dies verschafft dem Betreiberausschluss selbst in Szenario B eine vom Vertrag teilweise unabhängige gesetzliche Grundlage.

Vorzugswürdig gegenüber der reinen Auftragsverarbeitung durch ein einziges Rechtssubjekt bleibt gleichwohl eine Gestaltung, die die Trennung bereits in der Verantwortlichkeitsstruktur abbildet. Der Gesetzgeber hat für verteilte Verwaltungsinfrastrukturen bereits von der Möglichkeit einer ausdrücklichen gesetzlichen Verantwortlichkeitszuweisung Gebrauch gemacht (vgl. § 8a Abs. 4 OZG). Eine entsprechende spezialgesetzliche Regelung könnte für ZaPuK nicht nur die Verantwortlichkeit zuweisen, sondern die domänenübergreifende Zusammenführung der Metadaten ausdrücklich untersagen und damit den Betreiberausschluss verbindlich und gegenüber jedermann wirksam machen. Diese Empfehlung steht in engem Zusammenhang mit der Zuweisung der datenschutzrechtlichen Verantwortlichkeit im verteilten Betrieb (siehe 2.2) und der dortigen Empfehlung einer spezialgesetzlichen Grundlage.

d) Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Kommunikationsmetadaten bleiben trotz Ende-zu-Ende-Verschlüsselung und pseudonymer Adressierung personenbezogen und hochsensibel; ihr Schutz ist datenschutzrechtlich geboten und – bei Einordnung als Telekommunikationsdienst – vom Fernmeldegeheimnis vorgezeichnet. Die Grundentscheidung zur Metadatenreduktion ist der wirksamste und rechtlich vorzugswürdige Beitrag und wird bestätigt.
- Die getrennte Betreiberstruktur (ADR-1103), die bereichsspezifische pseudonyme Adressierung (ADR-1104, ADR-1105) und das Protokollierungsverbot für IP-Adressen

in der Bürgerdomäne verwirklichen die Nichtverkettbarkeit und sind konsequent umzusetzen. Sie sollten über die Anschlussbedingungen um ein ausdrückliches Zusammenführungs- und Querzugriffsverbot ergänzt werden (ADR-1145).

- Bei Personen in Doppelrollen darf die Zusammenführung der Postfächer beider Domänen nur clientseitig erfolgen. Eine serverseitige Verknüpfung sowie jede Ableitbarkeit der Organisationsadresse aus dem Bereichspseudonym der Privatperson sind auszuschließen und in den Anschlussbedingungen (ADR-1145) zu untersagen. Die Registrierung von Berufsträgern im Adressregister ist mit dem Verzicht auf ein Adressregister für Privatpersonen vereinbar, solange sie auf die berufliche Adresse beschränkt bleibt und diese nicht auf die private Bereichsadresse abbildbar ist.

- Beim Betrieb durch verschiedene Rechtssubjekte (Szenario A) trägt bereits die getrennte Verantwortlichkeit den Betreiberausschluss. Er sollte durch gespiegelte vertragliche Zusammenführungs- und Querzugriffsverbote, ein verbindliches technisches Regelwerk, Change-Control-Klauseln sowie die Aufnahme in ISMS und Datenschutz-Folgenabschätzung abgesichert werden.

- Beim Betrieb durch dasselbe Rechtssubjekt in Auftragsverarbeitung (Szenario B) genügt eine Offenlegungspflicht für Zusammenführungsweisungen nicht. Der Ausschluss ist primär technisch zu verankern: Der Verantwortliche darf keine Schnittstelle erhalten, die eine domänenübergreifende Verknüpfung ermöglicht (Art. 25 DSGVO). Ergänzend sind Change-Control-Klauseln vorzusehen; das Fernmeldegeheimnis (§ 3 Abs. 3 TDDDG) wirkt als vom Vertrag unabhängige gesetzliche Schranke.

- Zur dauerhaften und gegenüber jedermann wirksamen Absicherung des Betreiberausschlusses empfiehlt sich – dem Vorbild des § 8a Abs. 4 OZG folgend – eine spezialgesetzliche Verantwortlichkeitszuweisung, verbunden mit einem ausdrücklichen Verbot der domänenübergreifenden Zusammenführung von Kommunikationsmetadaten (vgl. 2.2).

- Der besondere Vertraulichkeitsbedarf spezifischer Beziehungen (Informanten, V-Personen, verdeckte Ermittler, publizistischer Quellenschutz) bestätigt zusätzlich die Notwendigkeit einer belastbaren, nicht nur vertraglich gestützten Trennung.

4. Rechenschaftspflicht

Kurzzusammenfassung. Die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) verpflichtet den Verantwortlichen, die Einhaltung der Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO nicht nur zu gewährleisten, sondern auch nachweisen zu können. Sie ist kein eigenständiger materieller Grundsatz, sondern eine übergreifende Nachweis- und Dokumentationspflicht, die die vorstehend behandelten Grundsätze flankiert und im Streit- oder Prüffall die Beweislage verbessern soll. Konkretisiert wird sie durch Art. 24 DSGVO (geeignete, zu überprüfende und zu aktualisierende technische und organisatorische Maßnahmen einschließlich Nachweis) und durch die besonderen Dokumentationspflichten der Verordnung, namentlich das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), die Datenschutz-Folgenabschätzung (Art. 35 DSGVO), die Wirksamkeitsprüfung der Sicherheitsmaßnahmen (Art. 32 Abs. 1 lit. d DSGVO) sowie die Dokumentation von Datenschutzverletzungen (Art. 33 DSGVO).

Für ZaPuK ist die Rechenschaft – wie schon Rechtmäßigkeit und Verantwortlichkeit – nicht einheitlich, sondern rollen- und vorgangsbezogen zu bestimmen. Die domänenagnostische Infrastruktur (ADR-0001) trägt die Rechenschaft für die fachliche Verarbeitung nicht selbst, muss sie aber ermöglichen und dokumentierbar machen; jede verantwortliche Stelle bleibt für Nachweise bezüglich ihrer eigenen Verarbeitung zuständig. Praktisch bedeutsam ist dreierlei: Erstens ist angesichts der massenhaften und teils höchst sensiblen Kommunikation sowie des Einsatzes neuer Technologie (Matrix, Ende-zu-Ende-Verschlüsselung, perspektivisch MLS) regelmäßig eine Datenschutz-Folgenabschätzung erforderlich. Sie lässt sich für die gemeinsamen Infrastrukturbestandteile als nachnutzbare „Baustein-Folgenabschätzung" zentral bereitstellen und bei spezialgesetzlicher Grundlage bereits im Gesetzgebungsverfahren erbringen (Art. 35 Abs. 1 Satz 2, Abs. 10 DSGVO; siehe 3.6.3 und 2.2). Zweitens setzt Rechenschaft eine klare Verantwortlichkeitszuordnung voraus; die im verteilten Betrieb bestehende Unsicherheit (siehe 2.2) ist – dem Vorbild des § 8a Abs. 4 OZG folgend – möglichst durch Rechtsvorschrift

aufzulösen. Drittens ist die architektonisch bereits angelegte Nachweisfähigkeit (revisionssichere Protokollierung administrativer Vorgänge, Kennzeichnung technischer Nutzer, signierte Nachweise, offene ADR-Dokumentation) fortzuführen und im Einklang mit Datenminimierung und Metadatenschutz zweckgebunden und fristgebunden auszugestalten.

4.1. Inhalt und Konkretisierung der Rechenschaftspflicht

Nach Art. 5 Abs. 2 DSGVO ist der Verantwortliche für die Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO verantwortlich und muss deren Einhaltung nachweisen können. Die Vorschrift verlangt damit über die materielle Rechtstreue hinaus einen Nachweis dieser Rechtstreue. Ziel ist, dass Betroffene und Aufsichtsbehörden einfacher überprüfen können, ob rechtmäßig verarbeitet wird; die Pflicht reagiert auf frühere Lücken bei der Dokumentation von Verarbeitungsvorgängen und dient der Verbesserung der Beweislage.[297] Sie gilt als eines der auslegungsbedürftigsten Gebote der Verordnung.[298]

Konkretisiert wird die Rechenschaftspflicht zunächst durch Art. 24 DSGVO. Danach hat der Verantwortliche unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie des Risikos geeignete technische und organisatorische Maßnahmen umzusetzen, um die verordnungskonforme Verarbeitung sicherzustellen und den Nachweis dafür erbringen zu können. Diese Maßnahmen sind erforderlichenfalls zu überprüfen und zu aktualisieren (Art. 24 Abs. 1 DSGVO). Maßstab ist damit ein risikobasierter Ansatz, wie ihn auch ErwGr. 74 DSGVO vorgibt.[299] In der Wahl der Dokumentationsmittel ist der Verantwortliche grundsätzlich frei; er hat aber das Risiko der Verarbeitung zu berücksichtigen, und bereits eine fehlende oder lückenhafte Dokumentation kann für sich genommen als Pflichtverletzung geahndet werden.[300]

Ergänzt wird die allgemeine Nachweispflicht durch die besonderen Dokumentationspflichten der Verordnung: das Verarbeitungstätigkeitsverzeichnis nach Art. 30 DSGVO, die Dokumentation der Datenschutz-Folgenabschätzung nach Art. 35 Abs. 7 DSGVO, die Dokumentation der

[297] Kramer, in: Auernhammer, 8. Aufl. 2024, Art. 5 DSGVO, Rn. 61.
[298] Kramer, in: Auernhammer, 8. Aufl. 2024, Art. 5 DSGVO, Rn. 57.
[299] Kramer, in: Auernhammer, 8. Aufl. 2024, Art. 5 DSGVO, Rn. 61.
[300] Kramer, in: Auernhammer, 8. Aufl. 2024, Art. 5 DSGVO, Rn. 65.

Sicherheitsmaßnahmen nach Art. 32 DSGVO, die Dokumentation von Datenschutzverletzungen nach Art. 33 DSGVO sowie – für einwilligungsgestützte Verarbeitungen – den Nachweis der Einwilligung nach Art. 7 Abs. 1 DSGVO.[301] Als anerkannte Nachweismittel benennt die Verordnung überdies genehmigte Verhaltensregeln (Art. 40 DSGVO) und Zertifizierungen (Art. 42 DSGVO), auf die sich der Verantwortliche zum Beleg seiner Pflichterfüllung stützen kann (Art. 24 Abs. 3, Art. 32 Abs. 3 DSGVO).

4.2. Zwei Ebenen der Rechenschaft in ZaPuK

Wie bei der Rechtmäßigkeit und der Verantwortlichkeit sind auch für die Rechenschaft zwei Ebenen zu unterscheiden. Auf der Ebene der fachlichen Verarbeitung schulden die kommunizierenden Stellen den Nachweis, dass ihre Verarbeitung der Nachrichteninhalte den Grundsätzen des Art. 5 Abs. 1 DSGVO entspricht; die Rechtsgrundlage und der Nachweis richten sich nach dem jeweiligen Fachrecht. Als domänenagnostische Infrastruktur ohne fachspezifische Logik (ADR-0001) kann ZaPuK diese Rechenschaft nicht vorwegnehmen, sondern muss sie ermöglichen und – etwa durch die im Exportpaket zusammengeführten Nachweisartefakte (ADR-1135) – unterstützen. Auf der Ebene des Infrastrukturbetriebs trifft die Rechenschaft die Backend-Betreiber für die von ihnen verarbeiteten Kommunikationsmetadaten sowie jede Stelle mit Klartextzugriff (Endgeräte, versendende Stellen, serverseitige Entschlüsselungsendpunkte).

Aus dem relativen Begriff des Personenbezugs (siehe 1.3) folgt eine Präzisierung: Hinsichtlich der nur als Chiffrat vorliegenden Nachrichteninhalte trifft die reinen Transport- und Speicherakteure keine inhaltsbezogene Rechenschaft, weil sie insoweit keine personenbezogenen Daten verarbeiten. Dies gilt allerdings nur, solange die Betreiber die Schlüssel lückenlos nicht erlangen können. Gerade dieser Umstand ist selbst Gegenstand der Rechenschaft: Der Betreiber muss die Provider-Blindheit – insbesondere die clientseitige Verschlüsselung eines etwaigen serverseitigen Schlüssel-Backups (siehe 3.6.2.e)) – nachweisen können, und er hat die zugrunde liegende Bewertung des Reidentifizierungsrisikos im Zeitverlauf zu überprüfen und zu dokumentieren (Krypto-Agilität; Art. 24 Abs. 1 Satz 2, Art. 35 Abs. 11 DSGVO). Die Rechenschaft wirkt damit nicht nur auf die datenschutzrechtlich regulierte Metadaten- und Klartextebene,

[301] Kramer, in: Auernhammer, 8. Aufl. 2024, Art. 5 DSGVO, Rn. 64.

sondern absichernd auch auf die Begründung der Nicht-Anwendbarkeit des Datenschutzrechts auf der Inhaltsebene.

4.3. Verzeichnis von Verarbeitungstätigkeiten

Zu den zentralen Nachweisinstrumenten gehört das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO; im JI-Bereich § 70 BDSG). Es ist von jedem Verantwortlichen für die in seine Zuständigkeit fallenden Verarbeitungen und von jedem Auftragsverarbeiter für die in seinem Auftrag durchgeführten Verarbeitungen zu führen (Art. 30 Abs. 1 und 2 DSGVO). In der verteilten ZaPuK-Struktur bedeutet dies, dass jeder Backend-Betreiber, jede teilnehmende Stelle und jeder eingeschaltete Dienstleister ein eigenes Verzeichnis führt. Die in Art. 30 Abs. 5 DSGVO vorgesehene Erleichterung für Einrichtungen mit weniger als 250 Beschäftigten greift praktisch nicht, weil die Verarbeitung im Verbund ein Risiko für die Rechte der betroffenen Personen birgt, nicht nur gelegentlich erfolgt und regelmäßig auch besondere Kategorien personenbezogener Daten betreffen kann; die Rückausnahme des Art. 30 Abs. 5 DSGVO ist damit erfüllt (dies gilt unabhängig von einer etwaigen künftigen Anhebung der Schwelle).

Für die Architektur folgt hieraus kein unmittelbarer Baustein, wohl aber ein Unterstützungsauftrag: Da das Verzeichnis unter anderem eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen verlangt (Art. 30 Abs. 1 lit. g DSGVO; § 70 Abs. 1 Nr. 9 BDSG) und diese Maßnahmen – Ende-zu-Ende-Verschlüsselung, pseudonyme Adressierung, Metadatentrennung, Löschregime – zentral vorgegeben sind, sollten zentral bereitgestellte Muster-Verzeichnisbausteine und TOM-Beschreibungen den teilnehmenden Stellen die Erfüllung dieser Pflicht erleichtern und zugleich eine einheitliche, belastbare Dokumentation im Verbund fördern.

4.4. Datenschutz-Folgenabschätzung

Die praktisch wichtigste Ausprägung der Rechenschaftspflicht ist für ZaPuK die Datenschutz-Folgenabschätzung. Sie ist durchzuführen, wenn eine Form der Verarbeitung – insbesondere bei Verwendung neuer Technologien – aufgrund von Art, Umfang, Umständen und Zwecken voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge

hat (Art. 35 Abs. 1 DSGVO). Für ein solches hohes Risiko sprechen bei ZaPuK mehrere der von der Verordnung und den Aufsichtsbehörden herangezogenen Kriterien: die umfangreiche Verarbeitung, die große Mengen personenbezogener Daten auf nationaler bzw. supranationaler Ebene und eine große Zahl betroffener Personen erfasst (ErwGr. 91 DSGVO; Auernhammer, Art. 35 DSGVO Rn. 91); die mögliche umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 35 Abs. 3 lit. b DSGVO) und ggf. der Einsatz neuer, jedenfalls aber komplexer und abzusichernder Technologien (Matrix-Protokoll, Ende-zu-Ende-Verschlüsselung, perspektivische MLS-Migration). Dass ein hohes Risiko nur in einem Teilbereich der Verarbeitung vorliegen muss,[302] verstärkt diesen Befund. Ergänzend sind die von den Aufsichtsbehörden nach Art. 35 Abs. 4 DSGVO veröffentlichten Muss-Listen heranzuziehen. Eine Datenschutz-Folgenabschätzung ist damit für die über ZaPuK abgewickelten Verarbeitungen regelmäßig erforderlich.

Inhaltlich verlangt die Folgenabschätzung eine systematische Beschreibung der Verarbeitung, eine Bewertung ihrer Notwendigkeit und Verhältnismäßigkeit, eine Risikobewertung sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen (Art. 35 Abs. 7 DSGVO). Hier findet die an mehreren Stellen dieses Gutachtens empfohlene dokumentierte Begründung ihren systematischen Ort: Die Wahl der Ende-zu-Ende-Verschlüsselung und ihres Terminierungspunkts, die Metadatenminimierung und die pseudonyme Adressierung sind als risikomindernde Garantien in der Folgenabschätzung darzustellen und zu begründen. Die Folgenabschätzung ist damit nicht nur Pflicht, sondern zugleich das Instrument, mit dem die architekturprägenden Grundentscheidungen als erforderlich und verhältnismäßig belegt werden.

Für die Verortung der Folgenabschätzung im Verbund sind zwei Erleichterungen bedeutsam. Zum einen erlaubt Art. 35 Abs. 1 Satz 2 DSGVO für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung; dies ermöglicht eine zentrale, referenzierbare Folgenabschätzung für die gemeinsamen Infrastrukturbestandteile, die die teilnehmenden Stellen für ihre eigene, auf den fachlichen Kontext bezogene Abschätzung nachnutzen können. Zum anderen kann nach Art. 35 Abs. 10 DSGVO auf eine erneute Einzel-

[302] Raum, in: Auernhammer, Art. 35 DSGVO, Rn. 9.

Folgenabschätzung verzichtet werden, soweit die Verarbeitung auf einer spezialgesetzlichen Grundlage beruht und bereits im Rahmen des Gesetzgebungsverfahrens eine Folgenabschätzung erfolgt ist. Dies ist ein zusätzliches Argument für die oben (siehe 3.6.3 und 2.2) empfohlene spezialgesetzliche Verankerung: Sie kann die einzelnen teilnehmenden Stellen von wiederkehrendem Abschätzungsaufwand entlasten. Schließlich verlangt Art. 35 Abs. 11 DSGVO eine Überprüfung bei Änderung des Risikos; die MLS-Migration und die fortlaufende Neubewertung des Reidentifizierungsrisikos sind hierfür die maßgeblichen Anlässe.

4.5. Nachweis der Wirksamkeit der Sicherheitsmaßnahmen

Die Rechenschaft erschöpft sich nicht in der Beschreibung der getroffenen Maßnahmen, sondern verlangt den Nachweis ihrer Wirksamkeit. Art. 32 Abs. 1 lit. d DSGVO fordert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Für ZaPuK deckt sich dies mit den Vorgaben des IT-Sicherheitsrechts, insbesondere mit der von der ITSiV-PV geforderten Prüfung exponierter Komponenten vor Produktivsetzung und dem Betrieb eines Informationssicherheits-Managementsystems (siehe IV). Als Baustein der Rechenschaft sind ferner die im Verbund vorgesehenen anlassbezogenen oder stichprobenartigen Konformitätsprüfungen zu verstehen (ADR-1145): Sie richten sich gezielt auf diejenigen Anschlussbedingungen, deren Einhaltung von außen nicht beobachtbar ist – namentlich die E2EE-Endpunkttreue, den Metadatenschutz und das Verhalten der Org-IdP-Adapter – und ergänzen damit die andernorts überwiegend strukturelle, technisch geprüfte oder erkennbare Zusicherung.

4.6. Technische Nachweisfähigkeit und ihr Verhältnis zur Datenminimierung

Die Zielarchitektur ist auf Rechenschaftsfähigkeit angelegt. Administrative Änderungen an Vorgangsräumen, Gruppen und Vertretungsregelungen werden revisionssicher protokolliert und sind einer natürlichen Person zuzuordnen (ADR-1102; SIC_NAC_NAC_005, ANF_FUN_ADR_070) und der technische Nutzer ist gegenüber den übrigen Teilnehmern als solcher zu kennzeichnen (ANF_FUN_IDE_047). Beides dient der Transparenz und der Nachvollziehbarkeit administrativer Eingriffe und trägt damit unmittelbar zur Rechenschaftsfähigkeit der jeweiligen Organisation bei. Die durchgängige und offene Dokumentation der Architekturentscheidungen im ADR-

Format bildet zusammen mit Schutzbedarfsfeststellung, Sicherheitskonzept und Datenschutz-Folgenabschätzung eine kohärente Nachweisgrundlage.

Von der Rechenschaftsfähigkeit zu unterscheiden – und mit ihr teils überschneidend – sind die zu Beweiszwecken bewusst erzeugten Nachweise, insbesondere die verpflichtende Bereitstellungsbestätigung (ADR-0018). Sie dient primär der Beweissicherung des Zugangs gegenüber Dritten und nicht der Rechenschaft; ihre unverschlüsselten Metadaten stärken zugleich aber die Nachvollziehbarkeit der Übermittlung. Für alle Protokoll- und Nachweisdaten gilt der bereits entwickelte Grundsatz: Die Rechenschaftspflicht rechtfertigt keine anlasslose Vorratsprotokollierung, sondern verlangt eine zweckgebundene, nach Datenart differenzierte und fristgebundene Ausgestaltung (siehe 3.5.2). Rechenschaft und Datenminimierung stehen damit nicht im Widerspruch, sondern sind im Wege einer risikoangemessenen Begrenzung in Ausgleich zu bringen.

4.7. Rechenschaft im verteilten Betrieb

Rechenschaft setzt eine klare Zuordnung der Verantwortlichkeit voraus. Solange – wie oben (2.2) dargestellt – nicht rechtssicher feststeht, ob im verteilten Betrieb getrennte oder gemeinsame Verantwortlichkeiten bestehen, bleibt auch der Adressat der Nachweispflicht unscharf. Es wird daher empfohlen, die Verantwortlichkeit dem Vorbild des § 8a Abs. 4 OZG folgend durch Rechtsvorschrift zuzuweisen; dies schafft zugleich Klarheit über die Rechenschaftspflichtigen. Wird eine gemeinsame Verantwortlichkeit begründet, ist in der Vereinbarung nach Art. 26 Abs. 1 DSGVO transparent festzulegen, wer welche Pflichten – einschließlich der Nachweis- und Informationspflichten – erfüllt. Wird der Betrieb einzelner Komponenten (etwa Raum-Management-Service und Berechtigungsverzeichnis im delegierten Betrieb, ADR-1103 Option B) im Auftrag übernommen, führt der Auftragsverarbeiter das Verzeichnis nach Art. 30 Abs. 2 DSGVO, während die Rechenschaft für die Verarbeitung bei der Organisation verbleibt.

Soweit über das Justiz-Backend zweckabhängig dem JI-Regime unterfallende Verarbeitungen erfolgen (siehe 1.2), ist zu beachten, dass § 47 BDSG die Rechenschaftspflicht nicht ausdrücklich als eigenständigen Grundsatz wiederholt. Sie wird im JI-Bereich vielmehr über die Dokumentations- und Kontrollpflichten verwirklicht, namentlich das Verzeichnis nach § 70 BDSG, die

Protokollierung nach § 76 BDSG und die technisch-organisatorischen Anforderungen einschließlich der Trennbarkeit nach § 64 BDSG. Die Architektur muss eine solche zweck- und fristgebundene Nachweisführung ermöglichen, ohne sie auf die nicht dem JI-Recht unterfallenden Verarbeitungen zu übertragen.

4.8. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die Rechenschaftspflicht trifft jede verantwortliche Stelle für ihre eigene Verarbeitung; die domänenagnostische Infrastruktur (ADR-0001) nimmt sie nicht vorweg, muss den Nachweis aber ermöglichen und dokumentierbar machen.

- Für die über ZaPuK abgewickelten Verarbeitungen ist regelmäßig eine Datenschutz-Folgenabschätzung erforderlich (Art. 35 Abs. 1 und 3 DSGVO). Es wird empfohlen, für die gemeinsamen Infrastrukturbestandteile eine zentrale, nachnutzbare „Baustein-Folgenabschätzung" bereitzustellen (Art. 35 Abs. 1 Satz 2 DSGVO) und die risikomindernden Grundentscheidungen (E2EE, Metadatenminimierung, Pseudonymität) dort zu begründen (Art. 35 Abs. 7 DSGVO).

- Eine spezialgesetzliche Verankerung (siehe 3.6.3 und 2.2) entlastet zugleich die Rechenschaft: Sie kann die Verantwortlichkeit klarstellen und über Art. 35 Abs. 10 DSGVO eine gesetzgeberische Folgenabschätzung ermöglichen, die wiederkehrenden Aufwand der teilnehmenden Stellen vermeidet.

- Die zentral vorgegebenen technischen und organisatorischen Maßnahmen sollten durch zentral bereitgestellte Muster-Verzeichnisbausteine und TOM-Beschreibungen unterlegt werden, um die Verzeichnispflicht (Art. 30 DSGVO; § 70 BDSG) der teilnehmenden Stellen zu erleichtern und eine einheitliche Nachweisführung zu fördern.

- Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig zu überprüfen (Art. 32 Abs. 1 lit. d DSGVO). Die risikobasierten Konformitätsprüfungen im Einzelfall (ADR-1145) sollten als Rechenschaftsbaustein für die von außen nicht beobachtbaren

Anschlussbedingungen (E2EE-Endpunkttreue, Metadatenschutz, Org-IdP-Adapter) beibehalten werden.

- Die revisionssichere Protokollierung administrativer Vorgänge und die Kennzeichnung technischer Nutzer (ADR-1102; ANF_FUN_ADR_070, ANF_FUN_IDE_047) sind fortzuführen. Die dabei anfallenden Protokolldaten sind zweckgebunden, nach Datenart differenziert und fristgebunden auszugestalten; die Rechenschaftspflicht rechtfertigt keine anlasslose Vorratsprotokollierung (siehe 3.5.2).

- Die Nachweisbarkeit der Provider-Blindheit – insbesondere die betreiberblinde Ausgestaltung des Schlüssel-Backups – und die fortlaufende Neubewertung des Reidentifizierungsrisikos (Krypto-Agilität, Art. 35 Abs. 11 DSGVO) sind ausdrücklich abzusichern; sie tragen zugleich die Einordnung der verschlüsselten Inhalte als für die Betreiber nicht personenbezogen (siehe 1.3).

- Verbindliche Nachweis-, Protokollierungs- und Dokumentationsanforderungen gegenüber Betreibern und teilnehmenden Stellen sind über die Anschlussbedingungen (ADR-1145) zu transportieren, ohne die eigenständige datenschutzrechtliche Verantwortung der jeweiligen Stelle zu verlagern.

5. Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

Kurzzusammenfassung. Art. 25 DSGVO verpflichtet den Verantwortlichen, die materiellen Datenschutzgrundsätze nicht erst im laufenden Betrieb, sondern bereits bei der Festlegung der Verarbeitungsmittel technisch und organisatorisch wirksam umzusetzen. Die Vorschrift hat zwei Ausprägungen: den Datenschutz durch Technikgestaltung (data protection by design, Art. 25 Abs. 1 DSGVO), der geeignete, am Stand der Technik und am Risiko ausgerichtete Maßnahmen bereits im Entwurf verlangt und dabei Pseudonymisierung und Datenminimierung ausdrücklich als Beispiele nennt, und die datenschutzfreundlichen Voreinstellungen (data protection by default, Art. 25 Abs. 2 DSGVO), nach denen durch Voreinstellung nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden dürfen. Dies betrifft ausdrücklich die Menge der Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit

(Art. 25 Abs. 2 Satz 2 DSGVO). Art. 25 DSGVO verschafft damit den bereits behandelten Grundsätzen – Datenminimierung, Zweckbindung, Speicherbegrenzung sowie Integrität und Vertraulichkeit – auf der Ebene des Systementwurfs Geltung.

Für ZaPuK ist Art. 25 DSGVO von zentraler Bedeutung, weil die architekturprägenden Grundentscheidungen der Sache nach nichts anderes sind als eine Umsetzung von privacy by design: die durchgängige Ende-zu-Ende-Verschlüsselung (ADR-0011, ADR-0012, ADR-1100), die bereichsspezifische pseudonyme Adressierung (ADR-1105), die Metadatenminimierung und Betreibertrennung (ADR-1103; Architekturkonzept, Abschnitt 5.4.11), der Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111), die selektive Offenlegung im Identitätsnachweis (ADR-1107) sowie die kryptografisch isolierten, berechtigungsgesteuerten Vorgangsräume (ADR-1102). Diese Entscheidungen werden durch Art. 25 DSGVO nicht nur gestützt, sondern rechtlich gefordert (mit Gestaltungsspielraum im Einzelnen). Zu beachten ist dabei, dass Adressat des Art. 25 DSGVO allein der Verantwortliche ist, nicht der zentrale Entwickler oder Hersteller der Infrastruktur. Die by-design-Vorgaben sind daher über die zentrale Entwicklung, das SDK und die Anschlussbedingungen so zu verankern, dass die verantwortlichen teilnehmenden Stellen ihnen genügen können. Außerdem ist das Gebot datenschutzfreundlicher Voreinstellungen (Abs. 2) konsequent auf die noch offenen Konfigurations- und Standardfestlegungen anzuwenden.

5.1. Inhalt und Regelungsgehalt des Art. 25 DSGVO

Der Grundsatz des Datenschutzes durch Technikgestaltung beruht auf der Vorstellung einer Komplementärbeziehung von Recht und Technik: Ein Mehr an technischer Vorsorge kann den rechtlichen Spielraum bei der Beurteilung der Zulässigkeit einer Verarbeitung erweitern, während die rechtlichen Vorgaben zugleich Art und Umfang der gebotenen technischen Maßnahmen bestimmen.[303] Art. 25 Abs. 1 DSGVO verlangt dementsprechend, dass der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die

[303] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 1.

notwendigen Garantien in die Verarbeitung aufzunehmen (Art. 25 Abs. 1 DSGVO). Erfasst ist damit der gesamte Lebenszyklus eines Produkts oder Dienstes. Die Maßnahmen sind bereits im Planungsstadium zu treffen und im Fortgang der Verarbeitung fortlaufend zu überprüfen.[304] Dies ist für eine ZaPuK als zu errichtende Infrastruktur der Anknüpfungspunkt: Die datenschutzrechtliche Weichenstellung erfolgt in der Architektur- und Entwurfsphase, nicht im späteren Betrieb.

Der Maßstab des Art. 25 Abs. 1 DSGVO ist – ebenso wie bei Art. 32 DSGVO – ein beweglicher: Zu berücksichtigen sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen (Art. 25 Abs. 1 DSGVO). Die inhaltliche Konturierung dieses Maßstabs – insbesondere die Anlehnung an die Technischen Richtlinien des BSI und den IT-Grundschutz sowie das Gebot der Krypto-Agilität – ist bereits im Abschnitt zur Sicherheit der Verarbeitung entfaltet worden; die dortigen Ausführungen gelten hier entsprechend. Art. 25 und Art. 32 DSGVO überschneiden sich, verfolgen aber unterschiedliche Blickrichtungen: Art. 32 zielt auf die Sicherheit der Verarbeitung, Art. 25 auf die technikgestaltende Verwirklichung sämtlicher Datenschutzgrundsätze – d.h. nicht nur der Sicherheit, sondern auch der Datenminimierung, der Zweckbindung, der Speicherbegrenzung und der Transparenz.

Art. 25 Abs. 2 DSGVO ergänzt diesen Systemdatenschutz um den Selbstdatenschutz durch Voreinstellungen. Durch Voreinstellung dürfen nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Zweck erforderlich ist. Die Verpflichtung erstreckt sich ausdrücklich auf die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (Art. 25 Abs. 2 Satz 1 und 2 DSGVO). Die Auswahl der Voreinstellungen unterliegt damit unmittelbar dem Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b DSGVO.[305] Systematisch handelt es sich bei Abs. 2 um einen Unterfall des Abs. 1, weil Voreinstellungen stets nur im Rahmen des zuvor geschaffenen Funktionsumfangs möglich sind; die Anforderungen an die Voreinstellungen sind deshalb bereits bei der

[304] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 9.
[305] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 24.

Programm- und Prozessgestaltung mitzudenken.[306] Besondere Bedeutung hat Art. 25 Abs. 2 Satz 3 DSGVO, wonach personenbezogene Daten durch Voreinstellung nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden dürfen. Die Voreinstellung hat sich am kleinstmöglichen Adressatenkreis zu orientieren, der von der betroffenen Person sodann aktiv erweitert werden kann.[307]

Art. 25 Abs. 3 DSGVO benennt schließlich die Zertifizierung nach Art. 42 DSGVO als Faktor, mit dem die Erfüllung der Anforderungen der Absätze 1 und 2 nachgewiesen werden kann. Damit verweist Art. 25 auf die Rechenschaftsdimension, ohne die eigenständige Verantwortung des Verantwortlichen zu mindern (Art. 42 Abs. 4 DSGVO). Dies wird im Abschnitt zur Rechenschaftspflicht aufgegriffen. Konkretisierende Auslegungshilfen bieten die Leitlinien des Europäischen Datenschutzausschusses zu Art. 25.[308]

5.2. Adressat der Pflicht und Bedeutung für die zentrale Entwicklung

Art. 25 DSGVO verpflichtet ausschließlich den Verantwortlichen. Weder der Hersteller einer Software noch der Entwickler oder Betreiber einer Infrastruktur ist unmittelbarer Adressat der Norm. Die Verordnung ermutigt Hersteller lediglich, die Grundsätze bei Entwicklung und Gestaltung ihrer Produkte zu berücksichtigen (ErwGr. 78 DSGVO). Ist der Verantwortliche zugleich Hersteller der eingesetzten Produkte, trifft ihn die Pflicht unmittelbar; andernfalls hat er ihr im Rahmen seiner Auswahlentscheidung Rechnung zu tragen.[309] Ein unmittelbarer Durchgriff auf den Hersteller – etwa über Gewährleistungs- oder Schadensersatzrecht – bleibt die Ausnahme, weil regelmäßig nur der Verantwortliche die für die Abwägung maßgeblichen Umstände der konkreten Verarbeitung kennt. Eine belastbare vertragliche Verankerung der by-design-Vorgaben setzt voraus, dass auch die Details der Verarbeitungsvorgänge Gegenstand der Vereinbarung sind, und scheidet beim Einsatz von Standardsoftware daher regelmäßig aus.[310]

[306] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 1, 23.
[307] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 26.
[308] EDSA, Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, Oktober 2020.
[309] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 23.
[310] Brüggemann, in: Auernhammer, 8. Aufl. 2024, Art. 25 DSGVO, Rn. 23, 31.

Diese Adressatenstellung ist für ZaPuK von struktureller Bedeutung. Die datenschutzprägenden Kernkomponenten – Postfach-Backend, SDK und Referenzimplementierung – werden zentral entwickelt und bereitgestellt (Architekturkonzept, Abschnitt 4.1). Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind jedoch, wie im Abschnitt zu den datenschutzrechtlichen Rollen dargestellt, die teilnehmenden Stellen und die Backend-Betreiber, nicht der zentrale Entwickler als solcher. Damit besteht die Gefahr einer Verantwortungslücke: Diejenige Stelle, die die technikgestaltenden Entscheidungen faktisch trifft, ist nicht die nach Art. 25 DSGVO verpflichtete, und die verpflichtete Stelle hat auf die zentral getroffenen Entwurfsentscheidungen nur begrenzten Einfluss.

Die Zielarchitektur löst dieses Spannungsverhältnis im Ansatz zutreffend, indem sie die datenschutzfreundlichen Eigenschaften in die zentral bereitgestellten Bausteine einbaut und über die Anschlussbedingungen verbindlich macht. Das SDK kapselt die Ende-zu-Ende-Verschlüsselung samt Schlüsselverwaltung und nimmt den anbindenden Stellen die fehleranfällige Eigenimplementierung ab (ADR-0009; Architekturkonzept, Abschnitt 5.2.2). Die Referenzimplementierung und die verpflichtenden Vorgaben der Anschlussbedingungen (ADR-1145) sorgen dafür, dass die by-design-Eigenschaften nicht zur Disposition der einzelnen teilnehmenden Stelle stehen. Aus Sicht des Art. 25 DSGVO ist dieser Ansatz vorzugswürdig, weil er den Verantwortlichen die Erfüllung ihrer Pflicht ermöglicht und erleichtert, ohne ihre Verantwortung zu verlagern: Der Verantwortliche erfüllt seine Auswahlpflicht, indem er eine Lösung nutzt, deren Datenschutzeigenschaften zentral gewährleistet und – über Anschlussbedingungen und perspektivisch Zertifizierung – nachweisbar sind. Zu empfehlen ist, die Datenschutzeigenschaften der zentralen Bausteine zu dokumentieren und den anbindenden Stellen als nachnutzbare Nachweisgrundlage bereitzustellen (siehe dazu 4).

5.3. Datenschutz durch Technikgestaltung in der ZaPuK-Architektur (Art. 25 Abs. 1 DSGVO)

Die Grundentscheidungen der Zielarchitektur verwirklichen den Datenschutz durch Technikgestaltung auf allen von Art. 25 Abs. 1 DSGVO erfassten Ebenen. Sie werden hier nicht erneut in der Sache gewürdigt – das ist in den Abschnitten zur Datenminimierung, zur Sicherheit der

Verarbeitung und zum Metadatenschutz geschehen –, sondern unter dem spezifischen Gesichtspunkt zusammengeführt, dass Art. 25 DSGVO ihre Verankerung bereits im Systementwurf verlangt.

Die durchgängige Ende-zu-Ende-Verschlüsselung mit Terminierung im Endgerät (ADR-0011, ADR-0012, ADR-1100) ist die zentrale by-design-Garantie. Sie setzt die Grundsätze der Vertraulichkeit und der Datenminimierung strukturell und nicht bloß organisatorisch um und bewirkt zugleich, dass die verschlüsselten Inhalte für die reinen Transport- und Speicherakteure mangels Schlüsselzugriffs nicht personenbezogen sind (siehe Abschnitt 1.3). Die bereichsspezifische pseudonyme Adressierung (ADR-1104, ADR-1105) verwirklicht die von Art. 25 Abs. 1 DSGVO ausdrücklich genannte Pseudonymisierung und die Nichtverkettbarkeit auf der Adressierungsebene. Der Verzicht auf ein zentrales Adressregister für Privatpersonen (ADR-1111) und die Metadatentrennung durch getrennte Betreiberstrukturen (ADR-1103; Architekturkonzept, Abschnitt 5.4.11) vermeiden bereits im Entwurf einen Datenbestand, dessen bloße Existenz zweckändernde Nutzungen und Profilbildung nahelegen würde.

Hervorzuheben ist die selektive Offenlegung im fachlichen Identitätsnachweis. Die Wahl des Formats SD-JWT VC (ADR-1106, ADR-1107) erlaubt es, dem Empfänger nur die für den jeweiligen Anwendungsfall zwingend benötigten Angaben zu präsentieren und alle übrigen zurückzuhalten. Dies ist ein Musterbeispiel für Technikgestaltung im Sinne des Art. 25 Abs. 1 DSGVO, weil die Datenminimierung nicht der Disziplin des Anwenders überlassen, sondern in das Nachweisformat selbst eingebaut wird. Die kryptografisch isolierten Vorgangsräume mit berechtigungsgesteuertem Zugriff (ADR-1102, ADR-1112) verwirklichen die Begrenzung der Zugänglichkeit, die Art. 25 Abs. 2 DSGVO ausdrücklich als Bezugsgröße benennt, bereits auf der Ebene der Raumarchitektur. Schließlich ist die Krypto-Agilität (ADR-0012, ADR-1144) Ausdruck der von Art. 25 Abs. 1 DSGVO geforderten fortlaufenden Ausrichtung am Stand der Technik über den gesamten Lebenszyklus.

Für die Umsetzung folgt daraus, dass die Festlegung des Nachweisschemas mit den je Anwendungsfall zwingend erforderlichen Pflichtangaben (ADR-1107) und die Ausgestaltung der Schlüsselwiederherstellung konsequent am Maßstab des Art. 25 DSGVO auszurichten sind. Für

die Schlüsselwiederherstellung bedeutet dies insbesondere, dass ein serverseitiges Schlüssel-Backup betreiberblind auszugestalten ist (clientseitige Verschlüsselung vor Ablage); dies ist zugleich Sicherheits-, Datenminimierungs- und Anwendbarkeitsanforderung (siehe 1.3 und 3.6). Das Architekturkonzept trägt dem Rechnung (Architekturkonzept, Abschnitt 5.4.13).

5.4. Datenschutzfreundliche Voreinstellungen in der ZaPuK-Architektur (Art. 25 Abs. 2 DSGVO)

Auf der Ebene der Voreinstellungen ist ZaPuK an den vier Bezugsgrößen des Art. 25 Abs. 2 Satz 2 DSGVO – Menge, Umfang, Speicherfrist und Zugänglichkeit – zu messen.

Hinsichtlich der Zugänglichkeit setzt die Architektur die Voreinstellung auf den kleinstmöglichen Adressatenkreis bereits strukturell um. Jeder Vorgang wird in einem eigenen, kryptografisch abgeschlossenen Raum bearbeitet, dessen Mitgliederkreis über das Berechtigungsverzeichnis gesteuert wird. Externe Kommunikationspartner sehen ausschließlich ihren eigenen Vorgang, und die aggregierte Postfachsicht ist nach Berechtigungen gefiltert (ADR-1102, ADR-1105). Damit ist der von Art. 25 Abs. 2 Satz 3 DSGVO adressierten Gefahr, dass Daten ohne Zutun der betroffenen Person einer unbestimmten Zahl von Personen zugänglich werden, bereits durch die Grundkonstruktion begegnet. Die für den Historienzugriff neu beitretender Bearbeitender vorgesehene Konfiguration der Sichtbarkeit auf shared (ADR-1102) steht hierzu nicht im Widerspruch: Der Adressatenkreis bleibt auf die über das Berechtigungsverzeichnis gesteuerte Bearbeitergruppe eines geschlossenen Raums begrenzt. Es handelt sich gerade nicht um eine Zugänglichmachung gegenüber einer unbestimmten Personenzahl, sondern um eine bewusst am Need-to-know der zuständigen Gruppe ausgerichtete Freigabe (vgl. ANF_FUN_ADR_063).

Hinsichtlich der Menge und des Umfangs verwirklicht die absendergesteuerte Erzeugung von Nachweisen den Default-Gedanken. Nachweise und die mit ihnen verbundenen zusätzlichen Metadaten werden nur dann erzeugt, wenn der konkrete Kommunikationszweck sie erfordert (ADR-1119). Abruf- und Lesebestätigungen sind freiwillig, werden verschlüsselt übertragen und lösen keine serverseitige Protokollierung aus (ADR-1118). Ein Identitätsnachweis ist nicht bei jeder Kommunikation vorzusehen, sodass für rein informelle Kommunikation oder

Beratung eine anonyme Nutzung möglich bleibt (ADR-1106). Diese Ausgestaltungen entsprechen der Vorgabe, dass die datenschutzfreundliche Voreinstellung das Minimum bildet und ein Mehr an Verarbeitung aktiv angefordert werden muss.

Hinsichtlich der Speicherfrist verlangt Art. 25 Abs. 2 DSGVO eine an der Erforderlichkeit ausgerichtete Voreinstellung. Insoweit ist auf den Abschnitt zur Speicherbegrenzung zu verweisen: Die vorgesehenen konfigurierbaren, nach Datenart differenzierten Löschfristen sind so voreinzustellen, dass ohne besondere Anordnung nicht länger als erforderlich gespeichert wird. Verkehrsdaten sind dem engeren Regime des § 9 TDDDG zu unterwerfen.

Eine Präzisierung ist mit Blick auf § 9 Abs. 1 OZG angezeigt, wonach die Einwilligung in die elektronische Bekanntgabe als erteilt gilt, sofern der Nutzer sie nicht ausschließt (Opt-out). Diese Konstruktion betrifft, wie im Abschnitt zur Rechtmäßigkeit dargelegt, die verwaltungsverfahrensrechtliche Zugangseröffnung und nicht eine datenschutzrechtliche Verarbeitungsvoreinstellung. Sie ist daher nicht am Maßstab des Art. 25 Abs. 2 DSGVO zu messen. Für die datenschutzrechtlich relevanten Voreinstellungen – insbesondere für optionale Funktionen mit erweitertem Datenanfall – bleibt es dabei, dass die datenschutzfreundliche Variante voreingestellt sein muss und eine Abweichung ein aktives Eingreifen voraussetzt. Werden datenschutzfreundliche Einstellungen deaktivierbar ausgestaltet, können ergänzende Aufklärungs- und Informationspflichten greifen.[311]

5.5. Technikgestaltung im Anwendungsbereich der JI-Richtlinie

Soweit über das Justiz-Backend zweckabhängig dem JI-Regime unterfallende Verarbeitungen erfolgen (siehe 1.2), tritt an die Stelle des Art. 25 DSGVO die nationale Umsetzung des Art. 20 JI-Richtlinie. § 71 BDSG entspricht Art. 25 DSGVO, verschärft ihn aber in zwei für ZaPuK bedeutsamen Punkten: Er spricht ausdrücklich von Datensparsamkeit und verpflichtet, Verarbeitung und Systemgestaltung an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten (§ 71 Abs. 1 Satz 3 BDSG); zudem sind Daten zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck

[311] Brüggemann, in: Auernhammer, 8. Aufl., 2024, Art. 25 DSGVO, Rn. 27.

möglich ist (§ 71 Abs. 1 Satz 4 BDSG). Ergänzend konkretisiert § 64 BDSG die technischen und organisatorischen Anforderungen und nennt in seinem Katalog ausdrücklich die Trennbarkeit zu unterschiedlichen Zwecken erhobener Daten (§ 64 Abs. 3 Nr. 14 BDSG) sowie die Erreichung mehrerer Kontrollziele durch Verschlüsselung nach dem Stand der Technik (§ 64 Abs. 3 Satz 2 BDSG).

Diese Wertungen bestätigen die Grundausrichtung der Architektur und lassen sich zugleich als Konkretisierung dessen heranziehen, was der Datenschutz durch Technikgestaltung auch außerhalb des JI-Rechts nahelegt. Die frühestmögliche, bereichsspezifische Pseudonymisierung (ADR-1105) und die getrennte Haltung der Datenbestände (ADR-1103) sind im JI-Bereich nicht nur zulässig, sondern als Gestaltungs- und Kontrollmaßnahme vorgezeichnet.

5.6. Nachweis durch Zertifizierung

Nach Art. 25 Abs. 3 DSGVO kann ein genehmigtes Zertifizierungsverfahren nach Art. 42 DSGVO als Faktor herangezogen werden, um die Erfüllung der by-design- und by-default-Anforderungen nachzuweisen. Für eine bereichsübergreifend genutzte Infrastruktur mit vielen verantwortlichen Stellen ist dies ein naheliegendes Instrument: Eine Zertifizierung der zentral bereitgestellten Bausteine – Postfach-Backend, SDK, Referenzimplementierung – könnte den anbindenden Verantwortlichen den Nachweis erleichtern, dass die von ihnen genutzte Lösung den Anforderungen des Art. 25 DSGVO genügt. Die Zertifizierung mindert allerdings nicht die eigene Verantwortung der teilnehmenden Stellen (Art. 42 Abs. 4 DSGVO). Sie ist ein Baustein der Rechenschaftspflicht (siehe 4). Solange datenschutzspezifische Zertifizierungsverfahren nicht verfügbar sind, treten an ihre Stelle die dokumentierte Umsetzung der by-design-Eigenschaften, die risikobasierten Konformitätsprüfungen der Anschlussbedingungen (ADR-1145) und die Datenschutz-Folgenabschätzung.

5.7. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Art. 25 DSGVO ist der maßgebliche rechtliche Anknüpfungspunkt dafür, dass die datenschutzprägenden Entscheidungen bereits in der jetzigen Architektur- und

Entwurfsphase getroffen werden. Die zentralen Grundentscheidungen – Ende-zu-Ende-Verschlüsselung, pseudonyme bereichsspezifische Adressierung, Metadatentrennung, Verzicht auf zentrale Register, selektive Offenlegung und Vorgangsraum-Isolierung – sind nicht nur zulässig, sondern als Umsetzung des Datenschutzes durch Technikgestaltung geboten und werden bestätigt.

- Da Adressat des Art. 25 DSGVO allein der Verantwortliche ist, die technikgestaltenden Entscheidungen aber zentral getroffen werden, sollten die Datenschutzeigenschaften in die zentral bereitgestellten Bausteine (SDK, Referenzimplementierung, Backend) eingebaut, dokumentiert und über die Anschlussbedingungen (ADR-1145) verbindlich gemacht werden. Dies ermöglicht den verantwortlichen teilnehmenden Stellen die Erfüllung ihrer Pflicht, ohne ihre eigene Verantwortung zu verlagern.

- Die Architekturentscheidungen sind am Maßstab des Art. 25 DSGVO auszurichten. Für den Identitätsnachweis sind die je Anwendungsfall zwingend erforderlichen Pflichtangaben eng zu definieren und das Nachweisschema hierauf zu beschränken (vgl. ADR-1107). Für die Schlüsselwiederherstellung ist eine betreiberblinde Ausgestaltung des Schlüssel-Backups erforderlich (so vorgesehen im Architekturkonzept, Abschnitt 5.4.13).

- Die datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DSGVO) sind konsequent umzusetzen: minimaler Adressatenkreis der Vorgangsräume, bedarfsgesteuerte statt pauschale Nachweiserzeugung (ADR-1118, ADR-1119), anonyme Nutzung als Default wo kein Identitätsnachweis erforderlich ist (ADR-1106) sowie an der Erforderlichkeit ausgerichtete, nach Datenart differenzierte Speicherfristen. Wo datenschutzfreundliche Einstellungen abweichend konfigurierbar sind, sind flankierende Hinweise vorzusehen.

- Im Anwendungsbereich des JI-Rechts sind die verschärften Vorgaben des § 71 BDSG (Datensparsamkeit, frühestmögliche Pseudonymisierung) und des § 64 BDSG (Trennbarkeit, Verschlüsselung) zu beachten. Die Architektur bildet diese Anforderungen

bereits strukturell ab und sollte die zweck- und trennungsbezogene Ausgestaltung für die dem JI-Recht unterfallenden Verarbeitungen nachweisbar halten.

- Zur Absicherung und Erleichterung des Nachweises sollte die Nutzung der Zertifizierung nach Art. 42 DSGVO für die zentralen Bausteine geprüft werden (Art. 25 Abs. 3 DSGVO). Bis dahin tragen die dokumentierte Umsetzung, die Konformitätsprüfungen der Anschlussbedingungen und die Datenschutz-Folgenabschätzung den Nachweis der by-design- und by-default-Konformität (siehe 4).

IV. IT-Sicherheitsrecht

Kurzzusammenfassung. Das IT-Sicherheitsrecht verpflichtet die an ZaPuK beteiligten Stellen, die Verfügbarkeit, Integrität und Vertraulichkeit der eingesetzten informationstechnischen Systeme durch technische und organisatorische Maßnahmen nach dem Stand der Technik zu schützen. Anders als das Datenschutzrecht, das an die Verarbeitung personenbezogener Daten anknüpft, knüpft das IT-Sicherheitsrecht an Systeme, Komponenten und Betreiber an; welches Regime für ZaPuK gilt, lässt sich daher nicht einheitlich, sondern nur betreiber- und komponentenbezogen bestimmen. Für ZaPuK greifen drei einander ergänzende Schichten: erstens das auf § 5 OZG beruhende, für den Portalverbund spezielle Regime der ITSiV-PV, das für die zentralen Postfach-Komponenten unmittelbar einschlägig ist; zweitens das mit der Umsetzung der NIS-2-Richtlinie neu gefasste BSIG, das für die Einrichtungen der Bundesverwaltung und für Betreiber kritischer Anlagen gilt; drittens die spezialgesetzlichen Sonderregime des Telekommunikations- und Vertrauensdiensterechts, soweit ein Postfach als Telekommunikationsdienst (siehe V) oder ein Backend-Betreiber als qualifizierter Vertrauensdiensteanbieter (siehe VII.1.3) einzuordnen ist. Alle Schichten verwenden denselben beweglichen Maßstab des Standes der Technik, der sich mit dem des Art. 32 DSGVO deckt (siehe III.3.6). Die architekturprägenden Grundentscheidungen von ZaPuK – durchgängige Ende-zu-Ende-Verschlüsselung, kryptografische Nachweise, Zero-Trust, Metadatenminimierung und Krypto-Agilität – erfüllen die zentralen Anforderungen dieser Regime. Als Ergänzung zu empfehlen ist vor allem die verbindliche Verankerung eines Informationssicherheitsmanagements, der Nachweis- und

Meldepflichten sowie die Absicherung der Lieferkette; diese Anforderungen sind über die ITSiV-PV und die Anschlussbedingungen (ADR-1145) zu transportieren.

1. Anwendbarer Rahmen und Prüfungsmaßstab

Das IT-Sicherheitsrecht ist in Deutschland nicht in einem einheitlichen Gesetz kodifiziert, sondern verteilt sich auf ein allgemeines Cybersicherheitsrecht (BSIG in der Fassung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes), auf sektor- und bereichsspezifische Sonderregime (u.a. § 165 TKG, eIDAS-VO, ITSiV-PV) sowie auf die datensicherheitsrechtlichen Vorgaben des Art. 32 DSGVO. Diese Regime überschneiden sich technisch erheblich, haben aber unterschiedliche Schutzrichtungen und Adressatenkreise; ihre gemeinsame Klammer ist der Maßstab des Standes der Technik.[312]

Der Stand der Technik ist ein bewusst dynamischer, technikoffener Rechtsbegriff. Er verweist nicht auf ein starres Anforderungsniveau, sondern auf den jeweils fortgeschrittenen, in der Praxis bewährten Entwicklungsstand von Verfahren und Einrichtungen, weil sich Technologien und Bedrohungslage rascher verändern, als das Recht sie abbilden kann.[313] Weil derselbe Maßstab sowohl das Datensicherheitsrecht (Art. 32 DSGVO) als auch das IT-Sicherheitsrecht prägt, kann insoweit auf den datenschutzrechtlichen Teil verwiesen werden. Auf die dortige Eröterung des Standes der Technik, insbesondere die Anlehnung an die Technischen Richtlinien des BSI und den IT-Grundschutz sowie an das Gebot der Krypto-Agilität wird verwiesen (siehe III.3.6).[314]

Für ZaPuK folgt aus der betreiber- und komponentenbezogenen Anknüpfung, dass die Anwendbarkeit der einzelnen Regime für jede Komponente und jeden Betreiber gesondert zu prüfen ist. Als domänenagnostische Kommunikationsinfrastruktur (ADR-0001) kann ZaPuK nicht vorwegnehmen, welches Regime eine konkret angebundene Stelle trifft. Die Architektur ist deshalb am jeweils höchsten in Betracht kommenden Schutzniveau auszurichten und muss

[312] Skierka-Canton, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2026, § 8, Rn. 8, 65.
[313] Skierka-Canton, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2026, § 8, Rn. 8.
[314] Skierka-Canton, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2026, § 8, Rn. 65.

die Erfüllung der Anforderungen ermöglichen und nachweisbar machen. Dies entspricht der bereits im Datenschutzteil entwickelten Linie.

2. IT-Sicherheit im Portalverbund (§ 5 OZG, ITSiV-PV)

Das für ZaPuK unmittelbar und flächendeckend einschlägige Regime ist die auf § 5 OZG beruhende ITSiV-PV. Sie gilt für die IT-Komponenten des Portalverbunds und die zur Anbindung genutzten Komponenten, verlangt Maßnahmen nach dem Stand der Technik, ein an der Leitlinie des IT-Planungsrats ausgerichtetes Informationssicherheitsmanagement, ein Sicherheitskonzept nach den BSI-Standards 200-1 bis 200-3 bzw. ISO/IEC 27001, Penetrationstests und Webchecks vor Anbindung. Außerdem wird ein IT-Notfallmanagement gefordert, das die Anforderungen der Leitlinie für die Informationssicherheit in der jeweils geltenden Fassung erfüllt (§ 2 Abs. 11 ITSiV-PV); somit ergibt sich ein indirekter Verweis auch auf den BSI-Standard 200-4 zum Business Continuity Management bzw. auf den Grundschutz-Baustein DER.4 Notfallmanagement.[315] Weil das Postfach nach § 2 Abs. 7 OZG eine IT-Komponente ist und in § 2 Abs. 6 ITSiV-PV ausdrücklich genannt wird, ist das zentrale ZaPuK-Postfach von diesem Regime erfasst. Der besondere Wert der ITSiV-PV liegt darin, dass sie ein für Bund und Länder einheitliches, unabdingbares Mindestniveau vorgibt (§ 5 Satz 2 und 3 OZG) und so die föderale Zersplitterung des übrigen IT-Sicherheitsrechts überbrückt.

Nach § 5 OZG legt das Bundesministerium des Innern die zur Gewährleistung der IT-Sicherheit erforderlichen Standards für die im Portalverbund und zu dessen Anbindung genutzten IT-Komponenten durch Rechtsverordnung fest. Ihre Einhaltung ist für alle Stellen verbindlich, die entsprechende IT-Komponenten nutzen, und von den Regelungen kann durch Landesrecht nicht abgewichen werden (§ 5 Satz 2 und 3 OZG). Auf dieser Grundlage konkretisiert § 2 Abs. 1 ITSiV-PV den Maßstab dahin, dass für den Portalverbund und die unmittelbar angebundenen Komponenten Maßnahmen nach dem Stand der Technik zu treffen sind. Nach § 2 Abs. 2 ITSiV-PV wird die Einhaltung des Standes der Technik vermutet, wenn die in der Anlage aufgeführten Technischen Richtlinien des BSI in der jeweils geltenden Fassung eingehalten werden. Für den

[315] Siehe zum IT-Notfallmanagement Ziffer 5.5 der Leitlinie Informationssicherheit, Stand 06.12.2018, Version 2.0, wonach Notfallmanagement-Prozesse gem. dem IT-Grundschutzstandard des BSI in der jeweils gültigen Fassung zu etablieren sind.

Portalverbund ist dies namentlich die Technische Richtlinie BSI TR-03172 „Portalverbund". Die Vermutungswirkung gilt bei Fortschreibung einer Richtlinie für zwei Jahre fort (§ 2 Abs. 2 Satz 3 ITSiV-PV). Die Regelungstechnik ist damit strukturell krypto- und technikagil angelegt und deckt sich mit dem Entwurfsprinzip der Krypto-Agilität (ADR-1144).

Die ITSiV-PV verlangt über den abstrakten Maßstab hinaus konkrete organisatorische Vorkehrungen, die für ZaPuK unmittelbar umzusetzen sind. Die genutzten IT-Komponenten müssen einem Informationssicherheitsmanagementsystem unterliegen, das die Vorgaben der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats umsetzt (§ 2 Abs. 4 ITSiV-PV), und einem IT-Notfallmanagement nach derselben Leitlinie (§ 2 Abs. 11 ITSiV-PV, der auf BSI-Grundschutz und somit auf BSI-Standard 200-4 bzw. Baustein DER.4 verweist). Die verantwortlichen Stellen haben ein IT-Sicherheitskonzept nach den BSI-Standards 200-1, 200-2 und 200-3 oder nach ISO/IEC 27001 zu erstellen und umzusetzen, mindestens die Standard-Absicherung nach BSI-Standard 200-2 (§ 2 Abs. 5 ITSiV-PV). Besondere Bedeutung hat § 2 Abs. 6 ITSiV-PV: Komponenten, die unmittelbar mit dem Internet verbunden sind, sowie alle Komponenten mit hohem oder sehr hohem Schutzbedarf in mindestens einem der Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit sind vor Anbindung an den Portalverbund einem Penetrationstest und einem Webcheck zu unterziehen; die Vorschrift nennt dabei ausdrücklich das Postfach, ferner Nutzerkonto, Bezahldienst und Datensafe. Diese Prüfungen sind spätestens nach drei Jahren oder bei größeren Änderungen zu wiederholen (§ 2 Abs. 7 ITSiV-PV). Angesichts des im Datenschutzteil festgestellten hohen bis sehr hohen Schutzbedarfs der über ZaPuK abgewickelten Kommunikation greift dieses Prüferfordernis für die zentralen Postfach-Komponenten. Es deckt sich zugleich mit der datensicherheitsrechtlichen Pflicht zur regelmäßigen Wirksamkeitsprüfung (Art. 32 Abs. 1 lit. d DSGVO)[316] und mit den im Verbund vorgesehenen Konformitätsprüfungen (ADR-1145).

Für die verteilte Betriebsstruktur von ZaPuK ist § 2 Abs. 12 ITSiV-PV zentral: Werden IT-Komponenten von Dienstleistern betrieben, bleibt die auslagernde Stelle für die Erfüllung der Anforderungen verantwortlich; die Umsetzung ist durch eine jährliche Eigenerklärung zu

[316] Hornung/Schindler, in: Hornung/Schallbruch IT-SicherheitsR-HdB, 2. Aufl. 2025, § 21, Rn. 114.

dokumentieren. Dies bestätigt die im Datenschutzteil zu den Betriebsmodellen entwickelte Wertung, dass der delegierte oder souveräne Betrieb (ADR-1103) die Verantwortung der jeweiligen Organisation nicht verlagert. Für mittelbar angebundene Komponenten öffentlicher Stellen genügt nach § 3 ITSiV-PV ein Sicherheitskonzept nach den BSI-Standards 200-1 bis 200-3 oder einem vergleichbaren, vom Land anerkannten Standard, mindestens die Basis-Absicherung nach BSI-Standard 200-2; BSI-Standard 200-4 (Business Continuity-Management) ist nicht Teil der von § 3 ITSiV-PV geforderten Maßnahmen. Damit ist ein abgestuftes, an der Nähe zum Portalverbund orientiertes Mindestniveau vorgegeben, das die zentralen Backends stärker bindet als bloß mittelbar angebundene Fachverfahren.

Zu beachten ist die beschränkte Anwendbarkeit der ITSiV-PV: Sie bindet die öffentlichen Stellen, die Portalverbund-Komponenten nutzen. Private Organisationen als Teilnehmer sind nicht unmittelbar Adressaten. Ihnen sind die entsprechenden Sicherheitsanforderungen über die Anschlussbedingungen aufzuerlegen (ADR-1145). Die parallele Regelungstechnik anderer Fachplattformen – etwa die Bindung der Steuerberaterplattform an die ITSiV-PV und an ein BSI-konformes Informationssicherheitsmanagement (§ 1 StBPPV) – zeigt, dass die ITSiV-PV als übertragbarer Referenzstandard auch außerhalb des engeren Portalverbunds herangezogen werden kann.

3. Cybersicherheitsrecht des Bundes (BSIG in der NIS-2-Fassung)

Kurzzusammenfassung. Mit dem NIS-2-Umsetzungsgesetz ist das BSIG vollständig neu gefasst worden und seit dem 6. Dezember 2025 in Kraft (BSI, Pressemitteilung vom 5. Dezember 2025). An die Stelle der früheren, KRITIS-zentrierten §§ 8a ff. BSIG a.F. tritt die einrichtungsbezogene Systematik der §§ 28 ff. BSIG mit den Risikomanagementpflichten der §§ 30, 31 BSIG. Für ZaPuK ist das BSIG betreiberbezogen einschlägig: Der Bund als Betreiber des Privatpersonen-Backends unterliegt als Einrichtung der Bundesverwaltung den für besonders wichtige Einrichtungen geltenden Pflichten (§ 29 BSIG); ob und welche weiteren Betreiber erfasst sind, hängt von ihrer Rechts- und Trägerform sowie einer möglichen Einordnung als kritische Anlage ab. Die zehn Mindestmaßnahmen des § 30 Abs. 2 BSIG – insbesondere Kryptokonzepte, Vorfallbewältigung, Backup und Wiederherstellung, Lieferkettensicherheit, Wirksamkeitsprüfung und

Multi-Faktor-Authentifizierung – spiegeln sich weitgehend in den bereits getroffenen Architekturentscheidungen.

3.1. Anwendungsbereich

Die NIS-2-Richtlinie bezieht erstmals Einrichtungen der öffentlichen Verwaltung ein; für die Zentralregierung (Bund) zwingend, für die regionale (Landes-)Ebene nach einem risikobasierten Ansatz und für die kommunale Ebene fakultativ.[317] Das BSIG setzt dies für den Bund um: Einrichtungen der Bundesverwaltung im Sinne des § 29 Abs. 1 BSIG – Bundesbehörden, öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung und weitere Körperschaften auf Bundesebene – sind nach § 29 Abs. 2 BSIG wie besonders wichtige Einrichtungen zu behandeln, sodass insbesondere die Risikomanagementpflicht des § 30 BSIG gilt. Der Bund als Betreiber des zentralen Privatpersonen-Backends (vgl. Architekturkonzept, Abschnitt 4.2.3.1) unterfällt damit dem § 30 BSIG.

Für die übrigen Betreiber ist die Einordnung differenziert. Kommunale Stellen und juristische Personen, an denen ausschließlich Länder oder Kommunen beteiligt sind und die im öffentlichen Auftrag Leistungen für die Verwaltung erbringen, sind vom BSIG ausgenommen, soweit sie durch vergleichbares Landesrecht reguliert werden (§ 28 Abs. 8 BSIG). Für sie gilt nicht das BSIG, sondern die jeweilige landesrechtliche NIS-2-Umsetzung. Für eine gemeinsame Bund-Länder-Trägerschaft – wie sie für den Betrieb der Organisations-Backends in Betracht kommt – ist die Zuordnung zur Bundesverwaltung nach § 29 BSIG nicht eindeutig und im Einzelfall zu klären. Die Ausnahme des § 28 Abs. 8 BSIG greift jedenfalls nicht, wenn der Bund beteiligt ist. Unabhängig von dieser Einordnung unterliegt der Betrieb stets der ITSiV-PV und – soweit BSIG oder Landesrecht anwendbar sind – einem im Wesentlichen gleichlaufenden Pflichtenprogramm.

Zwei weitere Anknüpfungen sind zu beachten: Erreicht das zentrale Postfach-Backend als bundesweite, massenhaft genutzte Kommunikationsinfrastruktur die durch Rechtsverordnung

[317] Bostelmann, in: Hornung/Schallbruch IT-SicherheitsR-HdB, 2. Aufl. 2025, § 25, Rn. 21, 159; ders./Fischer, aaO, § 13, Rn. 76.

(§ 56 BSIG, BSI-Kritisverordnung) festgelegten Schwellenwerte, kommt eine Einordnung als kritische Anlage in Betracht (§ 2 Nr. 22 BSIG i.V.m. § 2 Nr. 3 KRITIS-Dachgesetz). Dann treten die verschärften Anforderungen des § 31 BSIG hinzu, insbesondere die Pflicht zum Einsatz von Systemen zur Angriffserkennung (§ 31 Abs. 2 BSIG) sowie die mögliche Untersagung kritischer Komponenten (§ 41 BSIG). Wird ein Postfach als öffentlich zugänglicher Telekommunikationsdienst betrieben (siehe V), gilt vorrangig § 165 TKG; die §§ 30, 31 BSIG sind für diese Dienste nach § 28 Abs. 5 BSIG ausgeschlossen, um eine Doppelregulierung zu vermeiden. Wird ein Backend-Betreiber schließlich zum qualifizierten Vertrauensdiensteanbieter, um die Vermutungswirkung eines qualifizierten Zustelldienstes zu erlangen (siehe VII.1.3), ist er besonders wichtige Einrichtung (§ 28 Abs. 1 Nr. 2 BSIG) und unterliegt zusätzlich den Sicherheitsanforderungen der eIDAS-VO.

3.2. Risikomanagementmaßnahmen

Soweit das BSIG anwendbar ist, verlangt § 30 Abs. 1 BSIG geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zum Schutz von Verfügbarkeit, Integrität und Vertraulichkeit, deren Einhaltung zu dokumentieren ist. § 30 Abs. 2 BSIG konkretisiert dies in zehn Mindestmaßnahmen, die den Stand der Technik einhalten und auf einem gefahrenübergreifenden Ansatz beruhen sollen. Für ZaPuK sind diese Maßnahmen bereits weitgehend in der Architektur angelegt:

- Kryptokonzepte (§ 30 Abs. 2 Nr. 8 BSIG) entsprechen den PKI-Anforderungen und dem Schlüsselmanagement der Zielarchitektur (ADR-1144; Architekturkonzept, Abschnitt 5.4.13). Die dortige Ausrichtung an BSI TR-02102 und die Krypto-Agilität setzen diese Vorgabe um.

- Bewältigung von Sicherheitsvorfällen sowie Backup, Wiederherstellung und Krisenmanagement (§ 30 Abs. 2 Nr. 2 und 3 BSIG) korrespondieren mit dem IT-Notfallmanagement der ITSiV-PV und mit der Schlüsselwiederherstellung, die zugleich datenschutz- und zugangsrechtlich geboten ist (siehe III.3.6.2).

- Sicherheit der Lieferkette sowie Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung einschließlich Schwachstellenmanagement (§ 30 Abs. 2 Nr. 4 und 5 BSIG) betreffen die zentral entwickelten und bereitgestellten Bausteine, namentlich SDK und Referenzimplementierung (ADR-0007, ADR-0009). Der offene, quelloffene Entwicklungsprozess mit öffentlicher Fehlermeldung und Upstream-Beiträgen (Architekturkonzept, Abschnitt 4.1.4) unterstützt das Schwachstellenmanagement. Für eingesetzte Dritt- und Matrix-Komponenten ist die Lieferkettensicherheit fortlaufend zu bewerten.

- Konzepte zur Bewertung der Wirksamkeit der Maßnahmen (§ 30 Abs. 2 Nr. 6 BSIG) decken sich mit den Penetrationstests der ITSiV-PV und der Wirksamkeitsprüfung nach Art. 32 Abs. 1 lit. d DSGVO.

- Multi-Faktor- bzw. kontinuierliche Authentifizierung und gesicherte Kommunikation (§ 30 Abs. 2 Nr. 10 BSIG) werden durch die Authentisierung über externe Identitätsprovider, die Vertrauensniveaus und die durchgängige Ende-zu-Ende-Verschlüsselung verwirklicht (ADR-1106, ADR-1107).

Hinzu treten die Melde-, Registrierungs- und Nachweispflichten der §§ 32 ff. BSIG, die im Fall eines erheblichen Sicherheitsvorfalls (§ 2 Nr. 11 BSIG) greifen. Sie korrespondieren mit der in den Anschlussbedingungen bereits vorgesehenen Meldepflicht bei Sicherheitsvorfällen (ADR-1145) und sollten dort für alle Teilnehmer verbindlich ausgestaltet werden, unabhängig davon, ob der einzelne Betreiber selbst dem BSIG unterfällt.

3.3. Telekommunikations- und vertrauensdiensterechtliche Sonderregime

Soweit ein ZaPuK-Postfach als interpersoneller Telekommunikationsdienst einzuordnen ist (dazu V), verpflichtet § 165 TKG den Diensteerbringer zu angemessenen technischen Vorkehrungen nach dem Stand der Technik zum Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten (§ 165 Abs. 1 TKG) sowie zur Beherrschung der Sicherheitsrisiken für Netze und Dienste (§ 165 Abs. 2 TKG). Die Vorschrift nennt Verschlüsselung ausdrücklich als geeignete Maßnahme (§ 165 Abs. 2 Satz 2 TKG) und übernimmt für Betreiber, die zugleich besonders wichtige oder wichtige Einrichtungen sind, den Katalog der NIS-2-

Mindestmaßnahmen (§ 165 Abs. 2a TKG). Das TK-Sicherheitsregime bestätigt damit die verschlüsselte Grundausrichtung von ZaPuK und tritt für als Telekommunikationsdienst betriebene Postfächer an die Stelle der §§ 30, 31 BSIG (§ 28 Abs. 5 BSIG). Zu den metadatenschützenden Wertungen des Fernmeldegeheimnisses siehe III.3.6 und V.

Wird über den bloßen Nachrichtentransport hinaus die volle Vermutungswirkung eines qualifizierten Zustelldienstes angestrebt, sind zusätzlich die Sicherheitsanforderungen der eIDAS-VO an qualifizierte Vertrauensdienste zu erfüllen (Art. 24 eIDAS-VO). Die integritätssichernden Anforderungen des Art. 44 eIDAS-VO und ihre Beweiswirkung sind im Zusammenhang mit der beweissicheren Übermittlung dargestellt (siehe VII.1.3). Die eIDAS-VO geht insoweit über den allgemeinen Stand-der-Technik-Maßstab hinaus, als sie kryptografische Mechanismen zwingend vorschreibt.

3.4. Föderale Umsetzung, Umsetzungslücken und Durchsetzung

Das Cybersicherheitsrecht ist föderal zersplittert. Das BSIG bindet nach § 29 BSIG allein die Einrichtungen der Bundesverwaltung. Die Einrichtungen der Landes- und Kommunalverwaltung unterfallen ihm grundsätzlich nicht (§ 28 Abs. 8 BSIG), sondern der jeweiligen landesrechtlichen NIS-2-Umsetzung, die in mehreren Ländern noch aussteht oder erst im Entstehen ist. Für eine bundesweit genutzte, von Bund, Ländern, Kommunen und privaten Organisationen gemeinsam betriebene Infrastruktur wie ZaPuK entstünde daraus ein uneinheitliches Schutzniveau, wenn allein auf das jeweils anwendbare allgemeine IT-Sicherheitsrecht abgestellt würde.

Zwei Mechanismen gleichen diese Heterogenität aus. Erstens setzt die ITSiV-PV auf Grundlage des § 5 OZG ein für Bund und Länder einheitliches, durch Landesrecht nicht abdingbares Mindestniveau, das unmittelbar an die Nutzung der Portalverbund-Komponenten anknüpft und damit unabhängig von der einrichtungsbezogenen NIS-2-Zuordnung greift. Zweitens transportieren die Anschlussbedingungen (ADR-1145) die sicherheitsrelevanten Vorgaben verbindlich auch an diejenigen Teilnehmer, die weder dem BSIG noch der ITSiV-PV unmittelbar unterfallen – insbesondere an private Organisationen und an Betreiber dezentraler Backends. Der im Architekturkonzept gewählte risikobasierte Ansatz der Föderationskontrolle mit strukturellen, technisch geprüften, erkennbaren und vertraglichen Zusicherungen sowie

anlassbezogenen Konformitätsprüfungen ist aus IT-sicherheitsrechtlicher Sicht tragfähig, weil er das gebotene Schutzniveau durchsetzt, ohne die Anschlusshürden unverhältnismäßig zu erhöhen. Er sollte jedoch – dem Pflichtenkatalog des § 30 Abs. 2 BSIG und den Vorgaben der ITSiV-PV folgend – die Mindestanforderungen an ISMS, Sicherheitskonzept, Penetrationstests, Kryptokonzept, Vorfallmeldung und Nachweisführung ausdrücklich benennen.

Die Rolle des BSI ist dabei unterstützend und standardsetzend: Es entwickelt und veröffentlicht die für die Vermutungswirkung maßgeblichen Technischen Richtlinien (§ 3 Abs. 1 Nr. 10 und 27 BSIG), stellt der Bundesverwaltung praxisnahe Hilfsmittel zur Umsetzung des § 30 BSIG bereit (§ 3 Abs. 1 Nr. 17 BSIG) und erarbeitet Empfehlungen für Identifizierungs- und Authentisierungsverfahren (§ 3 Abs. 1 Nr. 26 BSIG). Eine enge Abstimmung mit dem BSI, insbesondere zur Fortschreibung der Technischen Richtlinie TR-03172 für den Portalverbund, ist daher zu empfehlen. Sie erschließt zugleich die Vermutungswirkung des § 2 Abs. 2 ITSiV-PV.

3.5. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Die zentralen Postfach-Komponenten unterfallen als IT-Komponenten des Portalverbunds unmittelbar der ITSiV-PV. Das Postfach ist in § 2 Abs. 6 ITSiV-PV ausdrücklich genannt. Die Anforderungen an ISMS (§ 2 Abs. 4 ITSiV-PV), Sicherheitskonzept nach BSI 200-1 bis 200-3 bzw. ISO/IEC 27001 (§ 2 Abs. 5 ITSiV-PV), Penetrationstests und Webchecks vor Anbindung (§ 2 Abs. 6 und 7 ITSiV-PV) sowie IT-Notfallmanagement (§ 2 Abs. 11 ITSiV-PV mit indirektem Verweis auf BSI 200-4 und DER.4) sind verbindlich umzusetzen. Die Ausrichtung an den Technischen Richtlinien des BSI erschließt die Vermutung der Stand-der-Technik-Konformität (§ 2 Abs. 2 ITSiV-PV).

- Soweit das BSIG betreiberbezogen anwendbar ist – für den Bund über § 29 BSIG gesichert –, sind die zehn Mindestmaßnahmen des § 30 Abs. 2 BSIG einzuhalten. Sie sind in der Zielarchitektur überwiegend angelegt (Kryptokonzept, Vorfallbewältigung, Backup/Wiederherstellung, Lieferkettensicherheit, Wirksamkeitsprüfung, Multi-Faktor-Authentifizierung) und werden dadurch bestätigt.

- Die Einordnung der einzelnen Backend-Betreiber (Bundesverwaltung, kritische Anlage, Telekommunikationsdienst, Vertrauensdiensteanbieter) ist im Zuge der Betreiberfestlegung gesondert vorzunehmen. Für eine mögliche KRITIS-Einstufung des zentralen Backends sind die Angriffserkennung (§ 31 Abs. 2 BSIG) und die Vorgaben zu kritischen Komponenten (§ 41 BSIG) einzuplanen.

- Die Verantwortung für die IT-Sicherheit verbleibt auch im delegierten und souveränen Betrieb bei der auslagernden Stelle (§ 2 Abs. 12 ITSiV-PV). Dies deckt sich mit den Betriebsmodellen des ADR-1103. Der Betrieb durch Dienstleister ist datenschutz- und sicherheitsrechtlich als Auftragsverarbeitung auszugestalten.

- Die föderale Zersplitterung des allgemeinen IT-Sicherheitsrechts ist über die einheitliche ITSiV-PV (§ 5 OZG) und die Anschlussbedingungen (ADR-1145) auszugleichen. Die Anschlussbedingungen sollten die Mindestanforderungen an ISMS, Sicherheitskonzept, Penetrationstests, Kryptokonzept, Meldepflichten und Nachweisführung ausdrücklich benennen und auch private Teilnehmer verbindlich binden, ohne deren eigene Verantwortung zu verlagern.

- Der quelloffene, an DevSecOps und Upstream-Beiträgen ausgerichtete Entwicklungsprozess (Architekturkonzept, Abschnitt 4.1.4) unterstützt die Anforderungen des § 30 Abs. 2 Nr. 4 und 5 BSIG hinsichtlich Lieferketten- und Schwachstellenmanagement. Die Sicherheit der eingesetzten Dritt- und Matrix-Komponenten ist fortlaufend zu bewerten und zu dokumentieren.

- Der Stand der Technik ist ein dynamischer Maßstab; die eingesetzten kryptografischen Verfahren sind an BSI TR-02102 und dem IT-Grundschutz auszurichten und krypto-agil zu halten (ADR-1144). Datensicherheits- und IT-sicherheitsrechtliche Maßnahmen sollten gemeinschaftlich betrachtet und nachgewiesen werden, um eine doppelte Prüfung zu vermeiden.

V. TK-Recht

Kurzzusammenfassung: Das Telekommunikationsrecht knüpft – anders als das Datenschutzrecht – nicht an die Verarbeitung personenbezogener Daten, sondern an das Erbringen eines Telekommunikationsdienstes an. Ob und in welchem Umfang es auf ZaPuK anwendbar ist, lässt sich daher nicht einheitlich, sondern nur dienst- und betreiberbezogen beantworten. Im Ausgangspunkt ist ein ZaPuK-Postfach seiner Funktion nach ein interpersoneller Telekommunikationsdienst, und zwar in der Ausprägung des nummernunabhängigen interpersonellen Telekommunikationsdienstes (§ 3 Nr. 24, Nr. 40 TKG). Auf die vom Europäischen Gerichtshof zur früheren Rechtslage für Web-E-Mail-Dienste noch verlangte Verantwortung für die Signalübertragung kommt es nach der Neufassung des TKG in Umsetzung des Europäischen Kodex für die elektronische Kommunikation nicht mehr an. E-Mail-, Messenger- und Gruppenchatdienste sind seither eigenständig erfasst.[318]

Die daraus folgenden Pflichten treffen ZaPuK gestuft. Das Fernmeldegeheimnis (§ 3 TDDDG) greift bereits deshalb, weil die Infrastruktur Telekommunikationsdienste geschäftsmäßig erbringt. Auf Entgelt, Gewinnerzielungsabsicht oder öffentliche Zugänglichkeit kommt es insoweit nicht an, sodass auch die staatlich betriebenen Backends erfasst sind (§ 3 Abs. 2 Nr. 2 TDDDG).[319] An das zusätzliche Erfordernis der öffentlichen Zugänglichkeit knüpfen demgegenüber die schärferen Sicherheitspflichten aus § 165 Abs. 2 ff. TKG samt ihren flankierenden Vorschriften (§§ 166 bis 169 TKG) sowie die Mitwirkungspflichten bei der Überwachung an. Anders als Absatz 1 erfasst dieser Pflichtenkreis nur, wer den Dienst selbst erbringt, nicht auch, wer an seiner Erbringung mitwirkt. Für die zentral betriebenen Backends ist beides zu bejahen; für ein souverän betriebenes Backend, das ausschließlich die Postfächer der eigenen Organisation bedient, ist es regelmäßig zu verneinen, ohne dass dies dessen Bindung an § 165 Abs. 1 TKG berührt.

[318] EuGH, Urteil vom 13.6.2019, C-193/18 – Google/Gmail; Hornung/Schindler, in: Hornung/Schallbruch IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 11; Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 34 f.

[319] Vgl. BT-Drs. 13/3609, S. 52; Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 38.

Aus der Einordnung als TK-Dienst folgen namentlich die Vertraulichkeits- und Metadatenpflichten des Fernmeldegeheimnisses, die strenge Zweckbindung und das Erfordernis der Löschung der Verkehrsdaten (§ 9 TDDDG), die Sicherungspflichten nach § 165 TKG sowie – bei öffentlich zugänglichen Diensten – Mitwirkungspflichten bei der Telekommunikationsüberwachung, die die Ende-zu-Ende-Verschlüsselung indes nicht in Frage stellen. Soweit ein Postfach zugleich als digitaler Dienst einzuordnen ist, treten die Pflichten des dritten Teils des TDDDG (insbesondere §§ 19, 25 TDDDG) hinzu. Im Verhältnis zur DSGVO sind die telekommunikationsrechtlichen Sonderregeln, soweit sie dieselben Pflichten betreffen, nach Art. 95 DSGVO vorrangig. Die architekturprägenden Grundentscheidungen – durchgängige Ende-zu-Ende-Verschlüsselung, Metadatenminimierung, pseudonyme Adressierung und Betreibertrennung – erfüllen die telekommunikationsrechtlichen Anforderungen und werden durch sie zusätzlich gestützt.

1. Anwendbarer Rahmen und Prüfungsmaßstab

Das für ZaPuK maßgebliche Telekommunikationsrecht verteilt sich auf zwei Regelwerke mit unterschiedlicher Schutzrichtung. Das TKG enthält die Begriffsbestimmungen und die markt-, sicherheits- und überwachungsbezogenen Pflichten. Das TDDDG regelt das Fernmeldegeheimnis und den kommunikationsbezogenen Datenschutz. Beide beruhen auf Unionsrecht – das TKG auf dem Europäischen Kodex für die elektronische Kommunikation (Richtlinie (EU) 2018/1972), das TDDDG in seinen kommunikationsschützenden Teilen auf der ePrivacy-Richtlinie (Richtlinie 2002/58/EG). Das TDDDG übernimmt die Begriffe des TKG und des DDG (§ 2 Abs. 1 TDDDG), sodass die telekommunikationsrechtliche Einordnung einheitlich anhand des TKG und die digitaldienstebezogene Einordnung anhand des DDG erfolgt.

Weil die Pflichten an den einzelnen Dienst und seinen Anbieter anknüpfen, ist die Anwendbarkeit – ähnlich wie im IT-Sicherheitsrecht – für jede Komponente und jeden Betreiber gesondert zu bestimmen. Als domänenagnostische Kommunikationsinfrastruktur (ADR-0001) kann ZaPuK nicht vorwegnehmen, welche Pflichten einen konkreten Betreiber treffen; Anbieter im telekommunikationsrechtlichen Sinne ist, wer den Dienst tatsächlich erbringt, also der jeweilige Betreiber des Postfach-Backends (im souveränen Betrieb die Organisation selbst, vgl. ADR-1103). Die

Architektur ist deshalb am jeweils höchsten in Betracht kommenden Pflichtenniveau auszurichten und muss dessen Erfüllung ermöglichen.

1.1. Einordnung des ZaPuK-Postfachs als Telekommunikationsdienst

Telekommunikationsdienste sind nach § 3 Nr. 61 TKG die in der Regel gegen Entgelt über Telekommunikationsnetze erbrachten Dienste; dazu zählen ausdrücklich die interpersonellen Telekommunikationsdienste (§ 3 Nr. 61 lit. b TKG). Ein solcher liegt vor, wenn der Dienst einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Beteiligten bestimmt werden (§ 3 Nr. 24 TKG). Diese Merkmale erfüllt ein ZaPuK-Postfach in seinem Kern: Es dient dem gezielten Austausch von Nachrichten und Dokumenten zwischen bestimmten Absendern und Empfängern und damit gerade nicht der Verbreitung an eine unbestimmte Öffentlichkeit. Es handelt sich auch nicht um eine bloß untergeordnete Nebenfunktion eines anderen Dienstes, die nach § 3 Nr. 24 a.E. TKG aus dem Begriff herausfiele; die Kommunikation ist vielmehr Hauptzweck der Infrastruktur.

Der Dienst ist nummernunabhängig. Nummerngebunden wäre er nur, wenn er zur Adressierung Nummern nationaler oder internationaler Nummernpläne verwendete oder die Kommunikation mit solchen Nummern ermöglichte (§ 3 Nr. 37 TKG). Die Verwendung sonstiger Kennungen genügt hierfür nicht.[320] ZaPuK adressiert über Matrix-Kennungen (MXID) und nicht über Rufnummern und fällt damit unter den nummernunabhängigen interpersonellen Telekommunikationsdienst (§ 3 Nr. 40 TKG). Das entspricht der Einordnung von E-Mail- und Messengerdiensten in Rechtsprechung und Literatur.[321]

Die frühere, für Web-E-Mail-Dienste ergangene Rechtsprechung steht dem nicht entgegen. Der Europäische Gerichtshof hatte den Dienst Gmail zur alten Rechtslage nicht als elektronischen Kommunikationsdienst eingestuft, weil der Anbieter nicht selbst die Verantwortung für

[320] Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 34.
[321] Hornung/Schindler, in: Hornung/Schallbruch IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 11; Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 35.

die Signalübertragung trage.[322] Mit der Einführung der eigenständigen Kategorie des interpersonellen Telekommunikationsdienstes durch den Europäischen Kodex und deren Umsetzung im TKG kommt es auf die Signalübertragung nicht mehr entscheidend an; die genannte Rechtsprechung ist insoweit überholt.[323]

Klärungsbedürftig sind für die staatlich getragene Infrastruktur zwei einschränkende Merkmale. Erstens verlangt § 3 Nr. 61 TKG einen in der Regel gegen Entgelt erbrachten Dienst. Das Merkmal wird unionsrechtlich weit verstanden und erfasst auch Dienste, für die der Nutzer kein Geld zahlt, aber Daten bereitstellt. Ob eine unentgeltliche, steuerfinanzierte und datensparsame Bereitstellung durch den Staat dieses Merkmal erfüllt, ist gleichwohl nicht zweifelsfrei. Zweitens knüpfen die schärferen Pflichten des TKG an die öffentliche Zugänglichkeit an, also an ein Angebot für einen unbestimmten Personenkreis (§ 3 Nr. 44 TKG). Das für alle Bürgerinnen und Bürger offene Privatpersonen-Backend ist öffentlich zugänglich; die Backends für Justiz und Behörden richten sich demgegenüber eher an einen bestimmten Nutzerkreis, sodass die öffentliche Zugänglichkeit dort im Einzelfall zu prüfen ist.

Für die praktisch wichtigste Folge – die Geltung des Fernmeldegeheimnisses – kommt es auf diese beiden Merkmale allerdings nicht an. Das Fernmeldegeheimnis verpflichtet auch den, der Telekommunikationsdienste ganz oder teilweise geschäftsmäßig erbringt (§ 3 Abs. 2 Nr. 2 TDDDG). Geschäftsmäßig ist bereits das nachhaltige, auf Dauer angelegte Angebot; auf eine Gewinnerzielungsabsicht kommt es nicht an, weshalb der Gesetzgeber ausdrücklich auch Nebenstellenanlagen in Behörden erfasst sieht.[324] Selbst wenn man ZaPuK mangels Entgelts oder öffentlicher Zugänglichkeit nicht als öffentlich zugänglichen Telekommunikationsdienst einordnete, unterliegt die Infrastruktur damit jedenfalls dem Fernmeldegeheimnis.

[322] EuGH, Urteil vom 13.06.2019, C-193/18 – Google/Gmail; ebenso zur Abgrenzung EuGH, Urteil vom 05.06.2019, C-142/18 – Skype/SkypeOut.
[323] Hornung/Schindler, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 11.
[324] BT-Drs. 13/3609, S. 52; Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 38.

1.2. Einordnung als digitaler Dienst und Doppelnatur

Die telekommunikationsrechtliche Einordnung schließt eine zusätzliche Qualifikation als digitaler Dienst nicht aus. Digitaler Dienst ist nach § 1 Abs. 4 Nr. 1 DDG ein Dienst der Informationsgesellschaft im Sinne des Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535, also ein in der Regel gegen Entgelt, elektronisch, im Fernabsatz und auf individuellen Abruf des Empfängers erbrachter Dienst. Der dritte Teil des TDDDG – der an die Stelle des früheren Telemedien-Datenschutzrechts getreten ist – knüpft seine Pflichten an diesen Begriff des digitalen Dienstes an und übernimmt ihn über § 2 Abs. 1 TDDDG. Während beim Telekommunikationsdienst die interpersonelle Signalübermittlung im Vordergrund steht, stellt der digitale Dienst auf die Vermittlung von Inhalten auf individuellen Abruf ab.[325]

Beide Einordnungen können nebeneinander bestehen (Doppelnatur). Der Unionsgesetzgeber geht ausdrücklich davon aus, dass bestimmte elektronische Kommunikationsdienste zugleich Dienste der Informationsgesellschaft sein können.[326] Der deutsche Gesetzgeber hat dies für nummernunabhängige interpersonelle Telekommunikationsdienste bestätigt.[327] Für ein ZaPuK-Postfach, das die Kommunikation über eine abrufbasierte, webgestützte Anwendung ermöglicht, liegt eine solche Doppelnatur nahe. Die Einordnung ist allerdings dienstbezogen vorzunehmen: Fasst ein Anbieter technisch und funktional unterschiedliche Leistungen zusammen, sind diese rechtlich getrennt zu bewerten.

Von der hier interessierenden datenschutzbezogenen Einordnung als digitaler Dienst nach dem TDDDG ist die inhalts- und aufsichtsbezogene Regulierung digitaler Dienste zu unterscheiden. Die medien-, plattform- und vermittlungsbezogenen Pflichten (etwa nach dem Digitale-Dienste-Gesetz zur Durchführung des Digital Services Act oder nach den medienrechtlichen Bestimmungen der Länder, § 1 Abs. 1 und 2 DDG) knüpfen an Vermittlungs-, Marktplatz-, Suchmaschinen- oder Hosting-Funktionen an. Ein ZaPuK-Postfach ist demgegenüber ein interpersoneller Kommunikationsdienst und kein solcher Vermittlungsdienst. Die genannten

[325] Hornung/Schindler, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 8.
[326] Erwägungsgrund 10 der Richtlinie (EU) 2018/1972.
[327] BT-Drs. 19/26108, S. 236 f.; Hornung/Schindler, in: Hornung/Schallbruch IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 8.

Pflichten treffen es daher im Regelfall nicht. Einschlägig ist vielmehr der datenschutzbezogene dritte Teil des TDDDG.

Aus der Einordnung als digitaler Dienst folgen für ZaPuK vor allem zwei Pflichtenkomplexe. Zum einen greifen die technischen und organisatorischen Vorkehrungen des § 19 TDDDG (Schutz gegen Kenntnisnahme Dritter, anonyme oder pseudonyme Nutzung, anerkanntes Verschlüsselungsverfahren nach dem Stand der Technik); sie werden im nachfolgenden Abschnitt 2 vertieft. Zum anderen ist § 25 TDDDG zu beachten: Die Speicherung von Informationen auf der Endeinrichtung der Nutzenden und der Zugriff auf dort bereits gespeicherte Informationen bedürfen grundsätzlich der Einwilligung (§ 25 Abs. 1 TDDDG), es sei denn, der Zugriff ist unbedingt erforderlich, um den vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen (§ 25 Abs. 2 Nr. 2 TDDDG). Für die zur reinen Diensterbringung erforderlichen Vorgänge – etwa die lokale Speicherung von Schlüsselmaterial und Nachrichten im Client – dürfte die Ausnahme greifen. Für darüber hinausgehende Zugriffe wäre eine Einwilligung einzuholen. Dieser Gesichtspunkt ist bei der Ausgestaltung der Postfachzugänge (Web- und App-Client) zu berücksichtigen.

2. Folgen der Einordnung als Telekommunikationsdienst

2.1. Fernmeldegeheimnis und Schutz der Kommunikationsbeziehung

Zentrale Folge ist die Geltung des Fernmeldegeheimnisses (§ 3 TDDDG). Es schützt den Inhalt der Telekommunikation und ihre näheren Umstände, ausdrücklich auch die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war (§ 3 Abs. 1 TDDDG). Den Verpflichteten ist es untersagt, sich über das für die Diensterbringung erforderliche Maß hinaus Kenntnis von Inhalt oder näheren Umständen des TK-Vorgangs zu verschaffen. Erlangte Kenntnisse dürfen nur zu diesem Zweck verwendet und nur weitergegeben werden, soweit ein Gesetz dies ausdrücklich und mit Bezug auf Telekommunikationsvorgänge vorsieht (§ 3 Abs. 3 TDDDG). Diese Bindung wirkt kraft Gesetzes und steht nicht zur Disposition eines Auftraggebers. Flankiert wird sie strafrechtlich durch § 206 StGB.[328]

[328] Dazu Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 86.

Für ZaPuK bestätigt dies die im datenschutzrechtlichen Teil entwickelte Linie in zweifacher Hinsicht. Hinsichtlich der Inhalte ist das Kenntnisverschaffungsverbot durch die durchgängige Ende-zu-Ende-Verschlüsselung strukturell bereits erfüllt, weil dem Betreiber der Klartext nicht zugänglich ist. Hinsichtlich der Kommunikationsmetadaten, die im Postfach-Backend zwangsläufig unverschlüsselt anfallen und trotz pseudonymer Adressierung dem Fernmeldegeheimnis unterfallen (§ 3 Abs. 1 TDDDG), begründet § 3 Abs. 3 TDDDG eine strikte Zweckbindung, die eine zweckwidrige Auswertung und insbesondere eine domänenübergreifende Zusammenführung untersagt. Das Fernmeldegeheimnis trägt damit den angestrebten Betreiberausschluss (dazu III.3.6.3) und verschafft ihm eine vom Vertrag unabhängige gesetzliche Grundlage. Die architektonischen Maßnahmen zur Metadatenreduktion, zur Betreibertrennung und zur bereichsspezifischen pseudonymen Adressierung (ADR-1103, ADR-1105) sind insoweit nicht nur datenschutzrechtlich, sondern auch telekommunikationsrechtlich geboten.

2.2. Verkehrsdaten und Störungsdaten

Für die bei der Diensterbringung anfallenden Verkehrsdaten gilt eine enge Zweckbindung. Sie dürfen nur zu den in § 9 Abs. 1 TDDDG abschließend genannten Zwecken – im Wesentlichen Aufbau und Aufrechterhaltung der Verbindung sowie Abrechnung – verarbeitet werden und sind im Übrigen nach Beendigung der Verbindung unverzüglich zu löschen. Eine darüber hinausgehende Verarbeitung ist unzulässig (§ 9 Abs. 1 Satz 2 und 3 TDDDG). Eine eigenständige, ebenfalls eng zweckgebundene Verarbeitung erlaubt § 12 TDDDG zum Erkennen, Eingrenzen und Beseitigen von Störungen. Auch dort sind die Daten unverzüglich zu löschen, sobald sie hierfür nicht mehr erforderlich sind (§ 12 Abs. 2 TDDDG). Für die Architektur folgt daraus, dass Verkehrsdaten von den Nachrichteninhalten und von den allgemeinen Betriebs- und Protokolldaten zu trennen und mit einem eigenen, an § 9 TDDDG ausgerichteten Löschregime zu versehen sind. Das über konfigurierbare Löschfristen vorgesehene Vorgehen (vgl. ADR-1135 sowie oben D.III.3.5) muss diese Trennung abbilden.

2.3. Nachrichtenübermittlung mit Zwischenspeicherung

Da ZaPuK Nachrichten bis zum Abruf verschlüsselt vorhält, ist § 6 TDDDG einschlägig, der die Verarbeitung zwischengespeicherter Nachrichteninhalte regelt und dem Endnutzer die

Bestimmung über Inhalt, Umfang und Zugriff zuweist (§ 6 Abs. 1 TDDDG). § 6 Abs. 2 TDDDG verlangt technische und organisatorische Maßnahmen nach dem Stand der Technik, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten auszuschließen. Diese Wertung deckt sich mit der Grundentscheidung für eine strikte Ende-zu-Ende-Verschlüsselung und mit der verbindlichen Adressregister-Prüfung vor Verwendung einer Rückantwortadresse (ADR-1111), die gerade Fehlübermittlungen verhindern soll.

2.4. Sicherheitspflichten nach dem TKG, ihr Adressatenkreis und das Verhältnis zum BSIG

§ 165 TKG unterscheidet zwei Pflichtenkreise mit unterschiedlichem Adressatenkreis (siehe 2.4.1). Absatz 1 verpflichtet jeden, der Telekommunikationsdienste erbringt oder daran mitwirkt, zu angemessenen Vorkehrungen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten; auf die öffentliche Zugänglichkeit kommt es nicht an. Die Absätze 2 ff. treffen demgegenüber nur, wer ein öffentliches Telekommunikationsnetz betreibt oder einen öffentlich zugänglichen Telekommunikationsdienst erbringt. Beide Einschränkungen sind für ZaPuK bedeutsam: Das bloße Mitwirken an der Erbringung genügt nicht, und der Dienst muss einem unbestimmten Personenkreis offenstehen.

Hieraus folgt, dass die Betriebsmodelle der Zielarchitektur unterschiedlich strengen TKG-Sicherheitspflichten unterliegen. Die zentral betriebenen Backends erbringen einen öffentlich zugänglichen Dienst und unterliegen dem vollen Pflichtenprogramm der Absätze 2 ff. sowie den daran anknüpfenden §§ 166 bis 169 TKG. Ein souverän betriebenes Backend, das ausschließlich die Postfächer der eigenen Organisation bedient, unterliegt dagegen nur Absatz 1; seine Teilnahme an der Föderation macht es nicht zum Anbieter des öffentlich zugänglichen Gesamtdienstes, sondern allenfalls zum Mitwirkenden.

Die schärfsten Pflichten des § 165 TKG – Zertifizierung kritischer Komponenten (Abs. 4), Verfügbarkeitssicherung (Abs. 5), turnusmäßiges Audit (Abs. 9 S. 2) und die anlasslose Vorlage des Sicherheitskonzepts (§ 166 Abs. 2 S. 1 TKG) – setzen den Betrieb eines öffentlichen Telekommunikationsnetzes voraus und scheiden für ZaPuK insgesamt aus, weil die Infrastruktur über das offene Internet erbracht wird und kein Netz betreibt.

2.4.1. Die abgestuften Pflichten des § 165 TKG

Nach Absatz 1 ist, „wer Telekommunikationsdienste erbringt oder daran mitwirkt", verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Dabei ist der Stand der Technik zu berücksichtigen. Der Adressatenkreis erfasst auch die nummernunabhängigen interpersonellen Telekommunikationsdienste;[329] zu denen das ZaPuK-Postfach gehört (siehe 1.1). Erfasst sind neben dem Anbieter auch Mitwirkende. Bloße Mitwirkende sind allerdings regelmäßig gegenüber dem primär verpflichteten Anbieter vertraglich gebunden (bei ZaPuK etwa über die Anschlussbedingungen). Die Pflicht zu Schutzmaßnahmen greift dann ihrem Sinn nach insoweit, wie sie über einen eigenständigen, vom Primärverpflichteten unabhängigen Handlungsspielraum verfügen und eigenverantwortlichen Zugriff auf die zu schützenden Daten erlangen.[330]

Nach Absatz 2 ist demgegenüber verpflichtet, „wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt". Der Verpflichtetenkreis unterscheidet sich damit in zwei Punkten von Absatz 1. Erstens muss der Dienst öffentlich zugänglich sein, also einem unbestimmten Personenkreis zur Verfügung stehen (§ 3 Nr. 44 TKG). Zweitens genügt das bloße Mitwirken an der Erbringung nicht, sondern nur das Betreiben beziehungsweise Erbringen selbst. Dies trägt dem unterschiedlichen Schutzzweck Rechnung. Während Absatz 1 dem Schutz der Betroffenen dient, verfolgen die Absätze 2 ff. ein öffentliches Interesse an der Funktionsfähigkeit der Infrastruktur.[331] Reine Mitwirkende ohne eigene Infrastruktur sind daher nicht erfasst.[332] Für das Merkmal des Erbringens gilt dabei das Gegenstück zur Funktionsherrschaft über ein Netz. Verpflichtet ist, wer die tatsächliche und rechtliche Kontrolle über den Dienst ausübt und in vergleichbarer Weise für dessen Funktionsfähigkeit einzustehen hat.[333]

---

[329] Ferner, in: BeckOK StPO, 60. Ed. 1.7.2026, TKG § 165, Rn. 3 f.
[330] Eckhardt, in: Geppert/Schütz, TKG, 5. Aufl. 2023, § 165, Rn. 17.
[331] Eckhardt, in: Geppert/Schütz, § 165, Rn. 1, 36 f.
[332] Eckhardt, in: Geppert/Schütz, § 165, Rn. 37; Mozek, in: Säcker/Körber, TKG–TTDSG, 4. Aufl. 2023, § 165, Rn. 16 f.
[333] Mozek, in: Säcker/Körber, § 165, Rn. 17.

2.4.2. Kern der strengeren Pflichten nach den Absätzen 2 ff.

Inhaltlich verlangt Absatz 2 angemessene technische und organisatorische Vorkehrungen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Netzen und Diensten führen – auch soweit sie auf äußere Angriffe oder Katastrophen zurückgehen –, sowie zur Beherrschung der Risiken für die Sicherheit von Netzen und Diensten. Satz 2 nennt Maßnahmen „einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung", um Systeme gegen unerlaubte Zugriffe zu sichern und die Auswirkungen von Sicherheitsverletzungen gering zu halten. Die Sätze 3 und 4 legen den Maßstab fest und verweisen auf den Stand der Technik, einschlägige europäische und internationale Normen sowie Umsetzungskosten einerseits, Risikoexposition, Größe des Anbieters sowie Eintrittswahrscheinlichkeit, Schwere und gesellschaftliche wie wirtschaftliche Auswirkungen von Sicherheitsvorfällen andererseits. Absatz 6 Satz 1 konkretisiert die Angemessenheit dahingehend, dass der technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Netze oder Dienste stehen darf. Verlangt wird damit ein an den üblicherweise zu erwartenden Gefährdungen ausgerichtetes gehobenes Standardniveau, nicht absolute Sicherheit.[334] Dieser Maßstab deckt sich grundsätzlich mit dem bereits im datenschutz- und IT-sicherheitsrechtlichen Teil dargelegten (siehe III.3.6 und IV).

Die Absätze 2a bis 2d übernehmen für Anbieter, die zugleich besonders wichtige oder wichtige Einrichtungen sind, den Katalog der NIS-2-Mindestmaßnahmen einschließlich Kryptographie- und Verschlüsselungskonzepten, Lieferkettensicherheit, Wirksamkeitsbewertung und Multi-Faktor-Authentifizierung sowie die Umsetzungs-, Überwachungs-, Haftungs- und Schulungspflichten der Geschäftsleitung. Eine Delegation an externe Dienstleister ist zulässig, entbindet die Leitung aber nicht von der fortlaufenden Überwachung.[335] Absatz 3 nennt als mögliche angemessene Maßnahme Systeme zur Angriffserkennung (§ 2 Nummer 41 des BSIG) und verpflichtet bei erhöhtem Gefährdungspotenzial zu ihrem Einsatz. Absatz 6 Satz 2 erklärt § 62 Abs. 1 BDSG für entsprechend anwendbar und stellt damit klar, dass die Einschaltung von

[334] Eckhardt, in: Geppert/Schütz, § 165, Rn. 54 f.; Säcker/Körber/Mozek, § 165, Rn. 28 f.
[335] Ferner, in: BeckOK StPO, TKG § 165, Rn. 15 f.

Auftragnehmern nicht befreiend wirkt.[336] Absatz 8 ermöglicht der Bundesnetzagentur bei Sicherheitsvorfällen oder erheblichen Gefahren die Anordnung von Abhilfemaßnahmen samt Fristen, Absatz 9 Satz 1 die Anordnung einer Überprüfung durch eine qualifizierte unabhängige Stelle. Durchgesetzt werden die Pflichten über § 183 TKG, der Anordnungen, Betretungsrechte, im Wiederholungsfall die ganze oder teilweise Untersagung des Dienstes (Abs. 4) und ein Zwangsgeld bis zu einer Million Euro (Abs. 5) vorsieht.

Flankiert wird § 165 TKG durch die §§ 166-169 TKG, die entsprechend für die Architektur relevant sind. § 166 TKG verlangt für den Betrieb öffentlicher TK-Netze oder die Erbringung eines öffentlichen TK-Dienstes einen Sicherheitsbeauftragten, einen in der Union ansässigen Ansprechpartner und ein Sicherheitskonzept, das die getroffenen und geplanten Schutzmaßnahmen darlegt. Für Diensteanbieter besteht keine anlasslose Pflicht zur Vorlage des Sicherheitskonzeptes bei der Bundesnetzagentur, diese kann die Vorlage aber verlangen (§ 166 Abs. 2 S. 2 TKG). Nach § 167 Abs 1 TKG legt die Bundesnetzagentur im Einvernehmen mit dem BSI einen Katalog von Sicherheitsanforderungen verbindlich fest, der „für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten" gilt. In dem Katalog wird auch bestimmt, wer als Anbieter mit erhöhtem Gefährdungspotenzial einzustufen ist (§ 167 Abs. 1 S. 1 Nr. 3 TKG). § 168 TKG etabliert (insbesondere für Erbringer öffentlich zugänglicher TK-Dienste) eine gestufte Meldekette bei erheblichen Sicherheitsvorfällen mit Erstmeldung binnen 24 Stunden, Meldung binnen 72 Stunden und Abschlussmeldung binnen eines Monats. § 169 TKG verpflichtet zur Benachrichtigung von Bundesnetzagentur und Bundesbeauftragtem bei einer Verletzung des Schutzes personenbezogener Daten und – bei schwerwiegender Beeinträchtigung – auch der Betroffenen. Bedeutsam ist die Ausnahme des § 169 Abs. 1 S. 3 TKG: Eine Benachrichtigung ist entbehrlich, soweit im Sicherheitskonzept nachgewiesen wurde, dass die betroffenen Daten durch geeignete technische Vorkehrungen, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens, gesichert waren. Die durchgängige Ende-zu-Ende-Verschlüsselung wirkt hier also nicht nur als Schutzmaßnahme, sondern als Privileg bzw. Ausnahme von der Melde- und Benachrichtigungspflicht – vorausgesetzt, sie ist im Sicherheitskonzept nach § 166 TKG

[336] Eckhardt, in: Geppert/Schütz, § 165, Rn. 56.

dokumentiert. Verstöße gegen die Vorlage- und Meldepflichten sind bußgeldbewehrt (§ 228 Abs. 2 Nr. 3 lit. c, Nr. 38 bis 41 TKG).

2.4.3. Was für ZaPuK von vornherein ausscheidet

Die intensivsten Pflichten knüpfen allein an den Betrieb eines öffentlichen Telekommunikationsnetzes an: die Vorabzertifizierung kritischer Komponenten (§ 165 Abs. 4 TKG), die Verfügbarkeitssicherung (§ 165 Abs. 5 TKG), das turnusmäßige Audit alle zwei Jahre (§ 165 Abs. 9 S. 2 TKG) und die unaufgeforderte Vorlage des Sicherheitskonzepts (§ 166 Abs. 2 S. 1 TKG). ZaPuK setzt als nummernunabhängiger interpersoneller Dienst auf der bestehenden Internetinfrastruktur auf. Die Übertragung leisten die Netzbetreiber, nicht die Postfach-Backends. Weder die zentralen noch die souverän betriebenen Backends sind daher Betreiber im Sinne des § 3 Nr. 7 TKG. Diese Pflichten scheiden für die Zielarchitektur insgesamt aus, dies gilt auch für die zentralen Backends.

2.4.4. Anwendung auf die Betriebsmodelle der Zielarchitektur

Für die zentral bereitgestellten Postfach-Backends (ADR-1103) ist die öffentliche Zugänglichkeit beim Privatpersonen-Backend eindeutig zu bejahen. Tendenziell dürften auch die Backends der Organisationen, öffentlichen Stellen und der Justiz als öffentlich zugänglich einzuordnen sei. Maßgeblich ist, ob die Leistung einem unbestimmten Personenkreis zugänglich ist, wie etwa ein Angebot „an jedermann".[337] Die zentralen Backends stehen einem im Voraus nicht individuell bestimmten Kreis von Organisationen und Stellen offen, deren Zugang von objektiven Anschlussvoraussetzungen abhängt. Dies könnte als „öffentlich zugänglich" eingeordnet werden, auch wenn diese Wertung nicht sicher ist. Vorsorglich sollten diese Backends als öffentlich zugängliche Telekommunikationsdienste behandelt werden. Anders liegt es beim souveränen Betrieb eines eigenen Backends (ADR-1103 Option C). Zwar greift auch hier ohne Weiteres § 165 Abs. 1 TKG, da der Betreiber den Dienst für die eigenen Postfächer selbst erbringt und eigenverantwortlichen Zugriff erlangt auf die zu schützenden Daten, namentlich auf die unverschlüsselt anfallenden Kommunikationsmetadaten. Dagegen

[337] BGH, Urteil vom 18.11.2021 – I ZR 106/20, Rn. 57 f.

greifen die Absätze 2 ff. regelmäßig aus zwei Gründen nicht. Zum einen fehlt es an der öffentlichen Zugänglichkeit. Der Dienst steht allein den Mitarbeitenden und Funktionspostfächern der betreibenden Organisation offen, also einer durch das Dienst- oder Mitgliedschaftsverhältnis klar abgegrenzten Personengruppe (ob dies bei einer hohen absoluten Zahl der Beschäftigten anders zu beurteilen sein kann, wäre von entsprechenden Betreibern ggf. zu prüfen). Zweitens erbringt der souveräne Betreiber den öffentlich zugänglichen Gesamtdienst des Verbunds nicht selbst, sondern wirkt daran lediglich mit. Das Mitwirken löst nach dem Wortlaut des Absatzes 2 keine Pflichten aus, wie der Umkehrschluss zu Absatz 1 zeigt. Das ist auch sachgerecht, weil der Mitwirkende die Sicherheit und Verfügbarkeit des Gesamtdienstes nicht steuern kann.

Beim delegierten Betrieb (ADR-1103 Option B) bleibt Anbieter des Dienstes der zentrale Betreiber. Die Organisation wirkt mit und unterliegt ebenfalls nur Absatz 1. Umgekehrt bleibt der zentrale Betreiber für die Absätze 2 ff. verantwortlich, auch soweit er sich Dritter bedient (§ 165 Abs. 6 S. 2 TKG in Verbindung mit § 62 Abs. 1 BDSG).

Insbesondere in zwei Konstellationen könnte die vorgenannte Einordnung kippen, was ggf. in den Anschlussbedingungen adressiert werden sollte. Dies betrifft Dienstleister, die Backends für eine im Voraus nicht bestimmte Zahl von Organisationen betreiben und damit am Markt auftreten, sowie ein souveränes Backend, das Postfächer für Personen außerhalb des eigenen Organisationskreises führt.

Zu beachten ist ferner § 165 Abs. 7 TKG: Bei gemeinsamer Nutzung technischer Einrichtungen trifft jeden Beteiligten die volle Pflicht, soweit sie sich nicht einem bestimmten Beteiligten zuordnen lässt.[338] Ob die gemeinsame Nutzung eines zentralen Backends darunterfallen kann, erscheint offen. Angesichts der Rechtsfolge empfiehlt sich eine ausdrückliche Zuordnung zum jeweiligen Betreiber in den Anschlussbedingungen (ADR-1145).

[338] Eckhardt, in: Geppert/Schütz, § 165, Rn. 61.

2.4.5. Verhältnis zum BSIG und Lücke in der Verweiskette

Für Einrichtungen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, gelten die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 BSIG nicht (§ 28 Abs. 5 S. 1 Nr. 1 BSIG). Das TKG-Regime tritt insoweit an die Stelle des allgemeinen Cybersicherheitsrechts.

Zu beachten ist allerdings, dass § 165 Abs. 2a bis 2d TKG den NIS-2-Katalog nicht unmittelbar anordnen, sondern an die Einstufung als besonders wichtige oder wichtige Einrichtung nach § 28 Abs. 1 S. 1 Nr. 3 beziehungsweise Abs. 2 S. 1 Nr. 2 BSIG anknüpfen. Von beiden Kategorien sind Einrichtungen der Bundesverwaltung ausgenommen (§ 28 Abs. 1 S. 2, Abs. 2 S. 2 BSIG). Für öffentlich getragene Stellen der Länder und Kommunen greift zudem § 28 Abs. 8 BSIG. Werden die zentralen Backends – wie vorgesehen – durch den Bund oder eine öffentlich getragene Stelle betrieben, läuft die Verweisungskette daher nach dem Wortlaut weitgehend leer. Praktische Folgen hat das kaum: Absatz 2 gilt unabhängig davon unmittelbar, und der Katalog des Absatzes 2a bleibt der maßgebliche Konkretisierungsmaßstab dafür, was gefahrenübergreifende Maßnahmen nach dem Stand der Technik sind. Hinzu treten die Anforderungen der ITSiV-PV. Es empfiehlt sich, den Katalog unabhängig von der formalen Einordnung zugrunde zu legen und dies im Sicherheitskonzept nach § 166 TKG zu dokumentieren.

2.5. Mitwirkung bei der Telekommunikationsüberwachung und Ende-zu-Ende-Verschlüsselung

Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat grundsätzlich technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen (§ 170 Abs. 1 TKG). Von dieser Pflicht befreit § 170 Abs. 4 TKG in Verbindung mit § 3 Abs. 2 Telekommunikations-Überwachungsverordnung (TKÜV) bestimmte Anlagen. Für ZaPuK sind vor allem zwei – jeweils größenabhängige – Befreiungstatbestände von Bedeutung: die allgemeine Freistellung von Anlagen mit höchstens 10.000 angeschlossenen Nutzern (§ 3 Abs. 2 Satz 1 Nr. 5 TKÜV) und die speziell für die hier maßgebliche Diensteart geltende Freistellung von Anlagen, mit denen ausschließlich nummernunabhängige

interpersonelle Telekommunikationsdienste erbracht werden und an die nicht mehr als 100.000 Nutzer angeschlossen sind (§ 3 Abs. 2 Satz 1 Nr. 6 TKÜV).

Bezugspunkt dieser Schwellenwerte ist nach dem Wortlaut die einzelne Telekommunikationsanlage – die Nutzer müssen „an sie" angeschlossen sein – und damit der jeweilige Anlagenbetreiber, dem die tatsächliche Kontrolle über die Funktionen der Anlage (Funktionsherrschaft) zukommt (§ 3 Abs. 1, § 2 Nr. 4 TKÜV.[339] Für die föderierte ZaPuK-Struktur spricht dies dagegen, auf die Gesamtzahl aller Verbundnutzer abzustellen; maßgeblich sind vielmehr grundsätzlich die Nutzer, die dem einzelnen Postfach-Backend zugeordnet (bei ihm registriert) sind, denn die Föderation ist eine Server-zu-Server-Vermittlung und begründet keinen „Anschluss" der Nutzer fremder Backends. Diese anlagenbezogene Lesart ist allerdings nicht gesichert: Der Begriff des „Anschlusses" passt auf nummernunabhängige, OTT-artige Dienste nur unvollkommen, und es ist nicht auszuschließen, dass die Bundesnetzagentur bei einem einheitlich als ZaPuK-Verbund auftretenden Gesamtdienst eine dienstbezogene, aggregierende Betrachtung anlegt, bei der die Schwelle praktisch stets überschritten wäre. Die Einordnung sollte daher mit der Bundesnetzagentur abgestimmt werden.

Selbst auf Grundlage der anlagenbezogenen Lesart führt die Schwelle für ZaPuK nur in engen Grenzen zu einer Befreiung. Die zentralen, bundesweit genutzten Backends – insbesondere das für alle Bürgerinnen und Bürger offene Privatpersonen-Backend – überschreiten die Schwelle von 100.000 Nutzern deutlich; für sie besteht die Vorhaltepflicht nach § 170 Abs. 1 TKG dem Grunde nach, soweit ein öffentlich zugänglicher Dienst vorliegt. Für Organisationen, die ein zentrales Backend nutzen (ADR-1103, Optionen A und B), ist zudem zu beachten, dass sie keine eigene Telekommunikationsanlage betreiben, sondern sich hierfür des zentralen Anlagenbetreibers bedienen (§ 170 Abs. 2 TKG). Maßgebliche Anlage ist dann im Zweifel das zentrale Backend, das die Schwelle überschreitet, sodass die Kleinanlagen-Befreiung für diese Organisationen von vornherein nicht greift. Ein eigenständiger Anwendungsbereich der Befreiung verbleibt damit im Wesentlichen für den souveränen Betrieb (Option C) einer einzelnen Organisation mit weniger als 100.000 (bzw. 10.000) zugeordneten Nutzern – und auch dort nur, soweit

[339] Heun, in: Auernhammer, 8. Auflage 2026, § 3 TTDSG, Rn. 79.

die anlagenbezogene Lesart trägt. Für Backends geschlossener Nutzergruppen (Justiz, Behörden) ist ohnehin vorab zu klären, ob überhaupt ein öffentlich zugänglicher Dienst und damit der Anwendungsbereich des § 170 TKG eröffnet ist; ist dies zu verneinen, entfällt die Vorhaltepflicht bereits im Ansatz.

Entscheidend ist, dass eine ggf. bestehende Vorhaltepflicht die Ende-zu-Ende-Verschlüsselung nicht in Frage stellt. Die Verpflichteten schulden nur die Ausleitung der bei ihnen tatsächlich vorliegenden Telekommunikation in der vorhandenen Form. Eine Pflicht, eine von den Kommunikationsparteien Ende-zu-Ende aufgebrachte Inhaltsverschlüsselung aufzuheben oder Entschlüsselungsmöglichkeiten (Hintertüren) vorzuhalten, besteht nicht. Das TKG verlangt die Aufhebung einer Verschlüsselung nur dort, wo der Verpflichtete sie selbst netzseitig aufgebracht hat (vgl. § 170 Abs. 11 TKG für das Mobilfunk-Roaming). Für die zentralen Backends bedeutet dies, dass sie im Rahmen einer Überwachungsanordnung die bei ihnen vorliegenden Chiffrate und die unverschlüsselten Kommunikationsmetadaten ausleiten, nicht aber den für sie ohnehin nicht zugänglichen Klartext. Die strikte, ausschließlich an den Endpunkten terminierende Verschlüsselung (ADR-0011, ADR-0012, ADR-1100) bleibt damit auch bei Bestehen von Überwachungspflichten tragfähig. Sie begrenzt lediglich den Kreis der ausleitbaren Daten auf das Chiffrat und die Metadaten.

3. Zusätzlich technische Vorkehrungen bei digitalen Diensten (§ 19 TDDDG)

Kurzzusammenfassung. Soweit ein Postfachzugang zugleich als digitaler Dienst einzuordnen ist, treten die technischen und organisatorischen Vorkehrungen des § 19 TDDDG hinzu, namentlich der Schutz gegen Kenntnisnahme Dritter (Abs. 1 Nr. 2), die Pflicht zur Ermöglichung einer anonymen oder pseudonymen Nutzung nebst Hinweispflicht (Abs. 2) und die Absicherung der technischen Einrichtungen nach dem Stand der Technik, für die das Gesetz die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens ausdrücklich nennt (Abs. 4).

Für ZaPuK begründet insbesondere die Pseudonymitätspflicht des Absatzes 2 keinen Handlungsbedarf. Sie ist nach überwiegender Auffassung auf das Auftreten gegenüber Dritten beschränkt und lässt die Identifizierung gegenüber dem Anbieter unberührt. Innerhalb des Postfachzugangs existiert eine solche Außendimension nicht, weil der Dienst keine dienstinterne

Sichtbarkeit zwischen Nutzenden vorsieht. Soweit die Nutzenden nach außen in Erscheinung treten, geschieht dies über die Telekommunikationsschicht (und dort ausschließlich unter bereichsspezifischen Pseudonymen). Die Vorschrift bestätigt damit die Architektur von der Zielrichtung, jedoch ohne ihr Vorgaben zu machen.

3.1. Gegenstand und Adressat der Pflicht

Digitaler Dienst im Sinne des § 1 Abs. 4 Nr. 1 DDG ist nicht die ZaPuK-Infrastruktur als Ganzes, sondern (allenfalls) der jeweils abrufbasiert bereitgestellte Postfachzugang, also der zentrale Postfachzugang als Web-Anwendung und mobile Anwendung, der Postfachbereich eines Fachportals und gegebenenfalls das Self-Service-Portal. Dies entspricht der oben dargestellten Doppelnatur: Die interpersonelle Signalvermittlung ist Telekommunikationsdienst, die darüberliegende, auf individuellen Abruf erbrachte Anwendungsschicht ist Dienst der Informationsgesellschaft. Die Matrix-Föderation, das Adressregister und der Application Service sind demgegenüber keine digitalen Dienste in diesem Sinne, weil sie keine Inhalte auf individuellen Abruf des Empfängers bereitstellen.

Ob bei ZaPuK insoweit überhaupt ein digitaler Dienst vorliegt, ist nicht eindeutig. Das Merkmal der „in der Regel entgeltlichen Erbringung“ verhindert ggf. die Anwendbarkeit. Anders als das Fernmeldegeheimnis, das über § 3 Abs. 2 Nr. 2 TDDDG bereits an das geschäftsmäßige Erbringen anknüpft, also weiter gefasst ist und deshalb auch die staatlich betriebenen Backends erfasst, setzt § 19 Abs. 1 bis 3 TDDDG über § 2 Abs. 1 TDDDG am Begriff des digitalen Dienstes und damit am Entgeltmerkmal an. Ob eine unentgeltliche, steuerfinanzierte hoheitliche Postfachanwendung dieses Merkmal erfüllt, ist offen. Das Merkmal wird unionsrechtlich weit verstanden, ob auch ein rein hoheitliches Angebot ohne wirtschaftlichen Hintergrund erfasst ist, ist jedoch offen.

Anbieter ist nach § 2 Abs. 2 Nr. 1 TDDDG jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zu ihnen vermittelt. Auf die datenschutzrechtliche Verantwortlichkeit kommt es nicht an, weil die Vorschrift nicht an die Verarbeitung personenbezogener Daten anknüpft. Maßgeblich ist die tatsächliche Verfügungsgewalt über die Hard- und Software, die den Dienst erzeugt, mithin die

Funktionsherrschaft.[340] Einen einheitlichen Anbieter gibt es für ZaPuK deshalb nicht. Verpflichtet ist jeweils die Stelle, die den konkreten Zugang bereitstellt, also der Bund für den zentralen Postfachzugang in Bundesportal und Deutschland-App, die zuständige Stelle für ein Fachportal und im souveränen Betrieb die Organisation für ihren eigenen Zugang.

3.2. Anwendbarkeit des § 19 Abs. 2 TDDDG neben der DSGVO

Ob § 19 Abs. 2 TDDDG neben der Datenschutz-Grundverordnung anwendbar ist, ist umstritten und gerade für diesen Absatz zweifelhaft. Die Vorschrift geht über § 13 Abs. 6 Telemediengesetz a.F. auf § 4 Abs. 6 TDDSG zurück und wurde bei der Übernahme in das TTDSG (jetzt TDDDG) nicht in den unionsrechtlichen Rahmen eingebettet.[341] Die Entwurfsbegründung geht pauschal davon aus, dass Teil 3 des Gesetzes nicht verdrängt werde.[342] Die Kommentierung differenziert demgegenüber absatzweise und hält Absatz 1 Alt. 1 für der Verordnung vorrangig sowie Absatz 1 Alt. 2 als Umsetzung des Art. 5 Abs. 1 ePrivacy-Richtlinie über Art. 95 DSGVO für gedeckt, während für Absatz 2 etwas anderes gelte, weil die dort verankerte Datenvermeidung ihre unionsrechtliche Entsprechung inzwischen im Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO gefunden habe. Für Absatz 1 Nr. 2 wird wegen Art. 32 Abs. 1 lit. b DSGVO teilweise sogar vollständige Unanwendbarkeit angenommen.[343] Höchstrichterlich ist die Frage ungeklärt; der BGH hatte in der Entscheidung zur Klarnamenpflicht nur die Rechtslage vor Geltung der Datenschutz-Grundverordnung zu beurteilen.[344] Für ZaPuK kann die Frage offenbleiben, weil sich aus der Vorschrift auch bei unterstellter Anwendbarkeit keine über die Architektur hinausgehende Anforderung ergibt.

3.3. Reichweite: kein Anwendungsgegenstand innerhalb des Postfachzugangs

Nach überwiegender Auffassung verpflichtet § 19 Abs. 2 TDDDG allein dazu, ein anonymes oder pseudonymes Auftreten im Verhältnis zu Dritten zu ermöglichen. Eine Pflicht, ein

[340] Schürmann, in: Auernhammer, 8. Auf. 2026, § 19 TTDSG, Rn. 19; Schindler, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 106.
[341] Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 2 f.
[342] BT-Drs. 19/27441, S. 36.
[343] Schindler, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2025, § 21, Rn. 100.
[344] BGH, Urteil vom 27.01.2022 – III ZR 3/21, Rn. 22.

Nutzungsverhältnis mit einer dem Anbieter selbst unbekannten Person einzugehen, folgt aus der Norm nicht; der Wortlaut erfasst nur die Nutzung und die Bezahlung, nicht die Anmeldung.[345] Auch der BGH ist davon ausgegangen, dass Nutzer dem Anbieter im Innenverhältnis ihren echten Namen mitteilen müssen und erst die anschließende Nutzung unter Pseudonym erfolgen kann.[346]

Dieses Begriffspaar ist am Beispiel sozialer Netzwerke entwickelt worden, bei denen die „Dritten" die übrigen Nutzenden desselben Dienstes sind, denen gegenüber Profil und Name sichtbar werden.[347] Eine solche dienstinterne Sichtbarkeit gibt es im Postfachzugang nicht. Der Dienst stellt kein Profil, kein Nutzendenverzeichnis und keine Selbstdarstellungsfunktion bereit. Für Privatpersonen ist ein Adressregister bewusst ausgeschlossen (ADR-1111). Jede nutzende Person sieht ausschließlich die eigenen Vorgänge. Soweit sie überhaupt nach außen in Erscheinung tritt, geschieht dies gegenüber den Kommunikationspartnern und damit auf der Telekommunikationsschicht, nicht innerhalb des digitalen Dienstes – und dort ausschließlich unter bereichsspezifischen, personenfreien Matrix-Adressen (ADR-1104, ADR-1105), ergänzt um den auf die erforderlichen Angaben beschränkten Identitätsnachweis (ADR-1106, ADR-1107).

Der von § 19 Abs. 2 TDDDG adressierte Regelungsgegenstand ist innerhalb des digitalen Dienstes damit nicht vorhanden. Legt man das Merkmal des Auftretens gegenüber Dritten funktional weiter aus und bezieht die über den Zugang vermittelte Kommunikation mit ein (was nach hier vertretener Auffassung zu weit geht), ist die Anforderung durch die pseudonyme Adressierung erfüllt und wird durch deren Bereichsspezifik sogar übererfüllt, weil zusätzlich die bereichsübergreifende Verkettbarkeit ausgeschlossen wird. Beide Lesarten führen zum selben Ergebnis. Hinzu kommt, dass die Vorschrift die anonyme und die pseudonyme Nutzung alternativ nebeneinanderstellt, sodass die Pseudonym-Variante genügt und die im Verwaltungsverfahren erforderliche Zurechenbarkeit der Pflichterfüllung nicht entgegensteht.

[345] Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 15.
[346] BGH, Urteil vom 27.01.2022 – III ZR 3/21.
[347] Vgl. Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 16, 18.

3.4. Grenzen des technisch Möglichen und Zumutbaren

Die Pflicht steht zudem unter dem Vorbehalt des technisch Möglichen und Zumutbaren. Technische Unmöglichkeit ist nach objektivem Maßstab zu bestimmen und liegt nur vor, wenn die Vorkehrung jedem Anbieter unmöglich ist. Die subjektiven Möglichkeiten des einzelnen Anbieters finden erst bei der Zumutbarkeit Berücksichtigung, die eine Abwägung unter Einbeziehung von Größe und Leistungsfähigkeit erfordert.[348] Eine vollständig anonyme Nutzung wird ohnehin verbreitet für nicht durchführbar gehalten, weil regelmäßig personenbezogene Kennungen wie die IP-Adresse verarbeitet werden müssen.[349]

Für ZaPuK kann sich insofern aus dem Ziel des sicheren Rechtsverkehrs eine gewisse Begrenzung der Zumutbarkeit ergeben. Unzumutbar und teilweise rechtlich ausgeschlossen ist die anonyme Nutzung dort, wo an die Identität der handelnden Person Rechtswirkungen anknüpfen. Der Gesetzgeber bringt dies mehrfach selbst zum Ausdruck. § 3a Abs. 2 Satz 3 VwVfG untersagt die Signierung mit einem Pseudonym, das der Behörde die Identifizierung nicht unmittelbar ermöglicht, und die Neufassung führt dieses Verbot in § 3b Satz 1 Nr. 2 VwVfG n.F. fort; § 3c Abs. 1 Nr. 2 VwVfG n.F. macht die Feststellung der Identität der erklärenden Person zur konstitutiven Voraussetzung eines sicheren Übermittlungswegs. § 8 Abs. 1 und 2 OZG regelt die Identitätsfeststellung im Nutzerkonto und § 9 Abs. 1 Satz 3 OZG verlangt den authentifizierten Abruf. Nicht tragfähig wäre demgegenüber die weitergehende Aussage, der sichere Rechtsverkehr schließe die Pseudonymität insgesamt aus. Eine solche Begründung liefe der Grundentscheidung der Zielarchitektur zuwider, die die pseudonyme Adressierung gerade deshalb für rechtssicher hält, weil die fachliche Identität nicht aus der Adresse abgeleitet, sondern über einen mit der Nachricht übermittelten Nachweis geführt wird (ADR-1104, ADR-1106, ADR-1111).

3.5. Kein verbleibender Handlungsbedarf

Die Hinweispflicht nach § 19 Abs. 2 Satz 2 TDDDG ist an die tatsächliche Möglichkeit einer anonymen oder pseudonymen Nutzung gekoppelt und entfällt, wenn der Dienst ohnehin nur

[348] Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 17 f., 53.
[349] Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 14, 53.

anonym oder pseudonym angeboten wird.[350] Das ist bei ZaPuK der Fall, weil die Adressierung natürlicher Personen durchgängig pseudonym erfolgt und keine Wahl zwischen pseudonymer und identifizierender Nutzung des Zugangs besteht. Die absendergesteuerte Entscheidung über die Beifügung eines Identitätsnachweises (ADR-1106, ADR-1119) betrifft den Inhalt der Kommunikation, nicht die Nutzung des digitalen Dienstes, und löst die Hinweispflicht daher nicht aus. Ein Transparenzhinweis in den Datenschutzhinweisen des Postfachzugangs bleibt gleichwohl sinnvoll.

Auch die für soziale Netzwerke diskutierte Frage einer formularmäßigen Klarnamenpflicht stellt sich nicht. Es kommt nicht darauf an, dass eine Klarnamenklausel in Nutzungsbedingungen ggf. gegen das gesetzliche Leitbild des § 19 Abs. 2 Satz 1 TDDDG verstoßen und nach § 307 Abs. 2 Nr. 1 BGB unwirksam sein kann.[351] Denn dieses Leitbild ist hier aufgrund des Vorstehenden nicht berührt. Auch beruht die Identifizierung bei ZaPuK nicht auf einer formularmäßigen Bestimmung, sondern auf gesetzlicher Anordnung (§ 8 Abs. 1 und 2, § 9 Abs. 1 Satz 3 OZG; künftig § 3c Abs. 1 Nr. 2 VwVfG).

Ein Merkposten verbleibt allein für künftige Funktionserweiterungen. Sollte ein Postfachzugang – etwa eine Drittimplementierung nach ADR-0003 – Verzeichnis-, Kontakt- oder Präsenzfunktionen einführen, die natürliche Personen gegenüber anderen Nutzenden sichtbar machen, entstünde eine dienstinterne Außendimension, für die § 19 Abs. 2 TDDDG dann Bedeutung erlangen könnte. Nach der derzeitigen Architektur ist dies nicht vorgesehen.

3.6. Folgerungen für die Architektur von ZaPuK

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Digitaler Dienst ist der jeweilige abrufbasierte Postfachzugang, nicht die Föderation, das Adressregister oder der Application Service. Verpflichtet ist die Stelle mit der

[350] Schürmann, in: Auernhammer, 8. Aufl. 2026, § 19 TTDSG, Rn. 19.
[351] Strittmatter, in: Schuster/Grützmacher, IT-Recht, 2. Aufl. 2025, § 662 BGB, Rn. 18.

Funktionsherrschaft über den Zugang; die Prüfung erfolgt zugangs- und betreiberbezogen.

- Ob § 19 Abs. 2 TDDDG durch die DSGVO verdrängt wird, kann offenbleiben, weil sich aus der Vorschrift jedenfalls keine zusätzliche Anforderung ergibt. Innerhalb des Postfachzugangs besteht keine Sichtbarkeit natürlicher Personen gegenüber anderen Nutzenden. Die Pflicht zur Ermöglichung pseudonymen Auftretens hat dort keinen Anwendungsgegenstand. Soweit die Nutzenden über die Telekommunikationsschicht nach außen treten, ist die Anforderung durch die bereichsspezifische pseudonyme Adressierung (ADR-1104, ADR-1105) erfüllt.

- Die Zumutbarkeitsgrenze des § 19 TDDDG trägt den Ausschluss der anonymen Nutzung für formgebundene und rechtswirksame Kommunikation (§ 3a Abs. 2 Satz 3 VwVfG, künftig § 3b Satz 1 Nr. 2 und § 3c Abs. 1 Nr. 2 VwVfG), nicht aber einen generellen Ausschluss der Pseudonymität. Auf ein solches Argument sollte nicht zurückgegriffen werden, da es der eigenen Grundentscheidung widerspräche.

- Eine Hinweispflicht nach § 19 Abs. 2 Satz 2 TDDDG besteht nicht, da der Zugang ohnehin ausschließlich pseudonym genutzt wird; ein Transparenzhinweis in den Datenschutzhinweisen bleibt empfehlenswert.

- Führen künftige Postfachzugänge Verzeichnis-, Kontakt- oder Präsenzfunktionen mit Sichtbarkeit natürlicher Personen ein, ist § 19 Abs. 2 TDDDG erneut zu prüfen. Die Anschlussbedingungen (ADR-1145) sollten die pseudonyme Adressierung als verbindliche Vorgabe absichern.

4. Verhältnis zur DSGVO

Soweit die telekommunikationsrechtlichen Sonderregeln denselben Gegenstand betreffen wie die DSGVO, gehen sie dieser nach Art. 95 DSGVO vor; die DSGVO erlegt insoweit keine zusätzlichen Pflichten auf. Das betrifft namentlich die Vertraulichkeit der Kommunikation und den Umgang mit Verkehrs- und Metadaten. Für den eigenständig neben dem Datenschutz stehenden Schutz des Fernmeldegeheimnisses wird teilweise vertreten, dass es auf den Vorrang des

Art. 95 DSGVO ohnehin nicht ankomme.[352] Im Ergebnis führt beides dazu, dass die kommunikationsschützenden Vorgaben des TDDDG bei der Ausgestaltung von ZaPuK vorrangig mitzudenken sind und die DSGVO ergänzend gilt.

5. Folgerungen für die Architektur von ZaPuK

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Ein ZaPuK-Postfach ist seiner Funktion nach ein nummernunabhängiger interpersoneller Telekommunikationsdienst (§ 3 Nr. 24, Nr. 40 TKG) und kann zugleich ein digitaler Dienst im Sinne des § 1 Abs. 4 Nr. 1 DDG sein (Doppelnatur). Die Architektur ist so auszulegen, dass sie den daran anknüpfenden Pflichten – insbesondere dem Fernmeldegeheimnis sowie den §§ 19, 25 DDG – genügt; die domänenagnostische Grundentscheidung (ADR-0001) steht dem nicht entgegen, verlangt aber eine betreiberbezogene Prüfung je Backend.

- Das Fernmeldegeheimnis (§ 3 TDDDG) greift wegen des geschäftsmäßigen Erbringens unabhängig von Entgelt und öffentlicher Zugänglichkeit und erfasst damit auch die staatlichen Backends. Es trägt den Schutz der Kommunikationsmetadaten und den Betreiberausschluss (siehe III.3.6.3) als gesetzliche, vom Vertrag unabhängige Schranke; die Metadatentrennung, die pseudonyme Adressierung und das Zusammenführungs- und Querzugriffsverbot (ADR-1103, ADR-1105, ADR-1145) sind hieran auszurichten.

- Verkehrsdaten sind von Inhalts- und allgemeinen Protokolldaten zu trennen und dem engen Regime der §§ 9, 12 TDDDG mit unverzüglicher, zweckgebundener Löschung zu unterwerfen. Das Löschfristenkonzept (ADR-1135) ist entsprechend zu differenzieren.

- Die Zwischenspeicherung (§ 6 TDDDG) und die technischen Vorkehrungen für digitale Dienste (§ 19 TDDDG) bestätigen die Ende-zu-Ende-Verschlüsselung, den Schutz

[352] Heun, in: Auernhammer, 8. Aufl. 2026, § 3 TTDSG, Rn. 44.

gegen Kenntnisnahme Dritter und die pseudonyme Nutzung; die verbindliche Adressregister-Prüfung vor Verwendung einer Rückantwortadresse (ADR-1111) dient zugleich dem Ausschluss von Fehlübermittlungen. Der Zugriff auf die Endeinrichtung (§ 25 TDDDG) ist auf das für die Diensterbringung unbedingt Erforderliche zu beschränken; darüberhinausgehende Zugriffe bedürfen der Einwilligung.

- § 165 Abs. 1 TKG bindet jeden Backendbetreiber, auch den souverän betreibenden, und zwar unabhängig von der öffentlichen Zugänglichkeit seines Dienstes. Die Pflicht zu angemessenen Vorkehrungen nach dem Stand der Technik zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten ist deshalb für alle Betriebsmodelle in den Anschlussbedingungen (ADR-1145) zu verankern.

- Die weitergehenden Pflichten der Absätze 2 ff. sowie der §§ 166 bis 169 TKG treffen nur die Betreiber der zentralen Backends (zur empfohlenen Anwendung der Absätze 2a ff. siehe 2.4.5). Für sie sind Sicherheitsbeauftragter, Ansprechpartner in der Union, Sicherheitskonzept und die gestufte Meldekette nach § 168 TKG einzuplanen. Das Sicherheitskonzept sollte mit dem nach der ITSiV-PV ohnehin geforderten Informationssicherheitsmanagement zusammengeführt werden, um Doppelstrukturen zu vermeiden.

- Souverän betriebene Backends, die ausschließlich Postfächer der eigenen Organisation führen, erbringen im Zweifel keinen öffentlich zugänglichen Dienst und wirken an der Erbringung des öffentlich zugänglichen Gesamtdienstes allenfalls mit. Die Absätze 2 ff. greifen daher nicht. Die Anschlussbedingungen sollten die entsprechenden Sicherheitsanforderungen für diese Betreiber vertraglich nachbilden, damit im Verbund kein uneinheitliches Schutzniveau entsteht, und zugleich klarstellen, dass die Öffnung eines Backends für organisationsfremde Postfächer die Einordnung ändert.

- Die Pflichten zur Zertifizierung kritischer Komponenten, zur Verfügbarkeitssicherung, zum turnusmäßigen Audit und zur anlasslosen Vorlage des Sicherheitskonzepts setzen den Betrieb eines öffentlichen Telekommunikationsnetzes voraus und scheiden

für ZaPuK aus, weil die Infrastruktur als Dienst auf der bestehenden Internetinfrastruktur aufsetzt.

- Die Ende-zu-Ende-Verschlüsselung kann über § 169 Abs. 1 S. 3 TKG als Ausnahme von der Meldungs- bzw. Benachrichtigungspflicht bei Verletzungen des Schutzes personenbezogener Daten gelten. Voraussetzung ist der Nachweis im Sicherheitskonzept. Die Verschlüsselungsarchitektur und das Schlüsselmanagement sind dort entsprechend zu dokumentieren.

- Bei gemeinsamer Nutzung der zentralen Backends durch mehrere Organisationen sollte die Zuordnung der Sicherheitspflichten ausdrücklich geregelt werden, um die Auffangregelung des § 165 Abs. 7 TKG und eine daraus folgende Gesamtverantwortlichkeit zu vermeiden.

- Für die Einordnung, ob die zentralen Backends als Anbieter mit erhöhtem Gefährdungspotenzial einzustufen sind, ist der Katalog der Bundesnetzagentur nach § 167 Abs. 1 S. 1 Nr. 3 TKG maßgeblich. Davon hängt insbesondere die Pflicht zum Einsatz von Systemen zur Angriffserkennung nach § 165 Abs. 3 S. 2 TKG ab. Die Einordnung sollte frühzeitig mit der Bundesnetzagentur geklärt werden.

- Bezugspunkt der TKÜV-Schwellen ist nach dem Wortlaut die einzelne Telekommunikationsanlage des jeweiligen Betreibers („an sie angeschlossen"), nicht der föderierte Gesamtdienst; ob die Bundesnetzagentur bei einem einheitlichen Verbunddienst aggregierend betrachtet, ist jedoch offen und sollte mit geklärt werden. Für die zentralen Backends (insbesondere das Privatpersonen-Backend) ist von einer TKÜ-Vorhaltepflicht nach § 170 Abs. 1 TKG auszugehen, da die 100.000-Nutzer-Schwelle klar überschritten wird. Organisationen, die ein zentrales Backend nutzen (Optionen A/B), können sich nicht auf die Kleinanlagen-Befreiung berufen, weil maßgebliche Anlage das große zentrale Backend ist (§ 170 Abs. 2 TKG); ein Anwendungsbereich der Befreiung verbleibt allenfalls für souveräne Einzelbetreiber (Option C) unterhalb der Schwellen. Angesichts dieser Unsicherheit sollte die Architektur die Vorhaltepflicht für den Verbund einplanen. Sie stellt die Ende-zu-Ende-Verschlüsselung nicht in Frage:

Auszuleiten sind nur die vorliegenden Chiffrate und Metadaten, eine Entschlüsselungs- oder Hintertürpflicht besteht nicht; die strikte Terminierung an den Endpunkten ist beizubehalten.

- Verbindliche telekommunikationsrechtliche Vorgaben gegenüber Betreibern und teilnehmenden Stellen – insbesondere zur zweckgebundenen Verkehrsdatenlöschung, zum Metadatenschutz und zur sicheren Ausgestaltung – sind über die Anschlussbedingungen (ADR-1145) zu transportieren, ohne die eigenständige Verantwortung des jeweiligen Betreibers zu verlagern.

- Wegen des Vorrangs nach Art. 95 DSGVO sind die kommunikationsschützenden Vorgaben des TDDDG bei der Ausgestaltung vorrangig zu berücksichtigen; die DSGVO gilt ergänzend.

VI. Einzelfragen zum Elektronischen Rechtsverkehr

1. Governance im Bereich Justiz

Für die Koordinierung der Zusammenarbeit bei der Planung, Errichtung und dem Betrieb informationstechnischer Systeme in der Justiz, die Entscheidung über grundlegende Fragen der Informations- und Kommunikationstechnik der Justiz und der IT-Projekte und die Festlegung von fachübergreifenden, justizspezifischen IT-Interoperabilitäts- und IT-Standards haben die Justizverwaltungen des Bundes und der Länder mit dem E-Justice-Rat ein eigenständiges Gremium eingerichtet.[353]

Bund und Länder üben ihre Zusammenarbeit gemäß Art. 91c Abs. 1 und 2 GG im Bereich der informationstechnischen Systeme der Justiz über dieses Gremium aus. Allerdings stellt der E-Justice-Rat die Mitwirkung der Justiz im IT-Planungsrat sicher. Eine Koordinierung der Arbeiten beider Gremien ist daher institutionell bereits angelegt.

[353] Siehe Bekanntmachung der Vereinbarung über die Errichtung des E-Justice-Rats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in der Justiz, Justizministerialblatt für das Land Brandenburg, Nr. 11, 15.11.2012, S. 107, abrufbar unter https://bravors.brandenburg.de/de/veroeffentlichungsblaetter_chronologisch/2012 (zuletzt abgerufen am 02.07.2026).

Im Bereich der Justiz existieren verschiedene Postfächer und Nutzerkonten, die im sog. EGVP-Verbund (Elektronisches Gerichts- und Verwaltungspostfach) zusammengeschlossen sind. Sie kommunizieren im Rahmen des durch die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach („ERVV") 2017 eingeführten Elektronischen Rechtsverkehrs, der auf Nutzung des OSCI-Protokolls beruht. An ZaPuK soll der EGVP-Verbund zunächst über ein zentrales Backend für Organisationen der Justiz und einen Protokollkonverter als externe Infrastruktur angeschlossen werden, sodass Anpassungen an den Systemen der Justiz nicht erforderlich sind.

Aus Sicht von ZaPuK ergeben sich allerdings bereits nach derzeitigem Stand verschiedene Einzelfragen insbesondere hinsichtlich der Kompatibilität der beiden Systeme.

2. Sicherungsniveau von Zugangsnachweisen im elektronischen Rechtsverkehr (fortgeschrittene versus qualifizierte Signatur/Zeitstempel/Siegel)

Vorbemerkung: Wie oben dargestellt, hängt die Frage, ob die Bereitstellung im Postfach Anknüpfungspunkt für den Zugang oder lediglich für den Eintritt einer Zugangsfiktion ist, vom Zugangs- bzw. Bekanntgabemodell ab sowie davon, ob das jeweilige Postfach als Machtbereich des Empfängers anzusehen ist (siehe im Einzelnen II.2.2). Zur besseren Lesbarkeit wird im Folgenden hinsichtlich des „Zugangsnachweises" nicht durchgängig zwischen den verschiedenen Konstellationen differenziert und der Begriff „Zugangsnachweis" untechnisch im Sinne des Nachweises des Eingangs bzw. der Bereitstellung im Postfach verwendet.

Kurzzusammenfassung. Das Recht des elektronischen Rechtsverkehrs kennt zwei verschiedene Bestätigungen, die sich nach der Übermittlungsrichtung unterscheiden. Bei der Einreichung an das Gericht erteilt dessen Empfangseinrichtung dem Absender die automatisierte Eingangsbestätigung nach § 130a Abs. 5 Satz 2 Zivilprozessordnung (ZPO). Sie entsteht auf der Gerichtsseite und ist von ZaPuK nicht zu erzeugen, sondern entgegenzunehmen. Bei der Zustellung durch das Gericht an nicht berufsmäßig Beteiligte knüpft § 173 Abs. 4 Satz 4 ZPO an diejenige automatisierte Eingangsbestätigung an, die der Eingang im vom Empfänger eröffneten Postfach auslöst. Sie entsteht auf der Empfängerseite und ist das funktionale Gegenstück zur

Bereitstellungsbestätigung nach ADR-0018, soweit das Postfach Machtbereich des Empfängers ist.

Für beide Bestätigungen gilt derselbe gesetzliche Mindeststandard: Weder ein qualifiziertes elektronisches Siegel noch ein qualifizierter elektronischer Zeitstempel ist vorgeschrieben. Die ERVV regelt Dateiformate, Übermittlungswege und Postfacharten, nicht aber die Sicherung von Quittungen. Die in ADR-0018 vorgesehene serverseitig signierte Bereitstellungsbestätigung erfüllt diesen Mindeststandard (und geht über das hinaus, was für die Bereitstellungsnachweise nach § 9 OZG und § 122a AO erforderlich ist).

Beweisrechtlich fällt die Antwort differenzierter aus: Für von einer Behörde befugt und „in der vorgeschriebenen Form" erstellte elektronische Dokumente („öffentliche elektronische Dokumente") greift nach § 371a Abs. 3 Satz 1 ZPO die Beweiskraft öffentlicher Urkunden bereits ohne qualifizierte Elemente, d.h. sie erbringen vollen Beweis darüber, dass die Erklärung vom Ersteller herrührt sowie für den beurkundeten Vorgang (§§ 415, 417, 418 ZPO). Lediglich die ergänzende Echtheitsvermutung des § 371a Abs. 3 Satz 2 ZPO iVm § 437 ZPO setzt eine qualifizierte Signatur oder – seit der Neufassung – ein qualifiziertes Siegel voraus. Für private elektronische Dokumente gilt dies nicht spiegelbildlich: Nach § 371a Abs. 1 ZPO erlangen diese die Beweiskraft privater Urkunden regelmäßig nur bei qualifizierter Signatur (das qualifizierte Siegel nennt die Vorschrift nicht).

Für ZaPuK ergeben sich daraus vier Empfehlungen: Die Serversignatur der Bereitstellungsbestätigung ist als fortgeschrittenes elektronisches Siegel mit Zertifikatsbindung an den Betreiber auszugestalten. Die Form der Bereitstellungsbestätigung sollte verordnungsrechtlich festgelegt werden, weil erst dies den Weg zur Urkundenbeweiskraft öffnet. Es sollte ein qualifizierter elektronischer Zeitstempel eingebunden werden (Architekturkonzept, Abschnitt 5.2.2), weil er das fristauslösende Element absichert und sich zentral bündeln lässt – der qualifizierte Zeitstempel verlangt nämlich nur ein fortgeschrittenes Siegel, allerdings eines qualifizierten Anbieters. Und die Clients müssen die gerichtsseitige Eingangsbestätigung nach § 130a Abs. 5 Satz 2 ZPO entgegennehmen, prüfbar anzeigen und speichern können.

2.1. Der prozessrechtliche Mindeststandard

2.1.1. Einreichung an das Gericht

Ein elektronisches Dokument ist eingegangen, sobald es auf der für den Empfang bestimmten Einrichtung des Gerichts gespeichert ist (§ 130a Abs. 5 Satz 1 ZPO). Nach Satz 2 ist dem Absender „eine automatisierte Bestätigung über den Zeitpunkt des Eingangs zu erteilen". Erzeugt wird sie nicht vom adressierten Gericht, sondern regelmäßig vom zentralen Intermediär der jeweiligen Landesjustizverwaltung, der sich in einem Rechenzentrum befindet. Das Risiko der Weiterleitung innerhalb der Justizinfrastruktur wird dem Absender damit bewusst abgenommen.[354]

Anforderungen an die kryptografische Sicherung dieser Bestätigung stellt das Gesetz nicht. Ihr Zweck ist begrenzt. Sie soll dem Absender unmittelbar und ohne Eingreifen eines Justizbediensteten Gewissheit über den Erfolg der Übermittlung verschaffen. Da sie automatisiert erteilt wird, enthält sie gerade keine Aussage über die Wirksamkeit des Eingangs oder die Einhaltung der Formvorschriften.[355] Der BGH behandelt sie funktional als Gegenstück zum Sendeprotokoll beim Telefax und stellt dabei ausschließlich auf den Inhalt der Meldung ab – maßgeblich sind der Meldetext „request executed" und der Übermittlungsstatus „erfolgreich" –[356] nicht auf ihre Signatur.[357]

Bemerkenswert ist gleichwohl, welche Angaben die Praxis aufnimmt. Die Musterdarstellung einer Eingangsbestätigung im EGVP-Kontext führt neben Nachrichtenkennzeichen, sekundengenauem Eingangszeitpunkt und Absender- sowie Empfängerdaten ausdrücklich das Signaturzertifikat des Empfangsservers auf.[358] Die Praxis geht damit über den gesetzlichen Mindeststandard hinaus, ohne dass daraus eine Rechtspflicht folgte.

---

[354] Loos, in: BeckOK IT-Recht, 22. Ed. 2026, § 130a ZPO, Rn. 32.
[355] Loos, in: BeckOK IT-Recht, 22. Ed. 2026, § 130a ZPO, Rn. 33; Kießling, in: Saenger, 10. Aufl. 2023, § 130a ZPO, Rn. 4.
[356] Vgl. BGH, Beschluss vom 11. Mai 2021 – VIII ZB 9/20; BGH, Beschluss vom 30. März 2023 – III ZB 13/22.
[357] Loos, in: BeckOK IT-Recht, 22. Ed. 2026, § 130a ZPO, Rn. 33.
[358] Loos, in: BeckOK IT-Recht, 22. Ed. 2026, § 130a ZPO, Rn. 33c.1.

Für ZaPuK ist entsprechend abzugrenzen: In dieser Übermittlungsrichtung erzeugt die Infrastruktur den Nachweis nicht. Er entsteht in der Justizinfrastruktur und ist über den Protokollkonverter (ADR-0010) entgegenzunehmen. Die Bereitstellungsbestätigung nach ADR-0018 deckt diesen Weg nicht ab, weil das empfangende Backend hier das Gericht beziehungsweise die EGVP-Infrastruktur ist.

2.1.2. Zustellung durch das Gericht an nicht berufsmäßig Beteiligte

Für die G2C-Konstellation gilt § 173 Abs. 4 ZPO. Die Zustellung setzt die Zustimmung des Empfängers voraus, die mit der Einreichung eines elektronischen Dokuments im jeweiligen Verfahren auf einem sicheren Übermittlungsweg als erteilt gilt (Satz 1 und 2). Der Wortlaut spricht bezüglich für eine unwiderlegliche gesetzliche Fiktion der Zustimmung, während die Gesetzesbegründung eher eine widerlegbare Vermutung nahelegt.[359]

Satz 4 knüpft die Zustellfiktion an „den auf der automatisierten Eingangsbestätigung ausgewiesenen Tag des Eingangs in dem vom Empfänger eröffneten elektronischen Postfach". Diese Bestätigung entsteht auf der Empfängerseite und wird an das Gericht beziehungsweise den sonstigen Absender zurückgemeldet. Sie gibt exakt an, wann das Dokument an das besondere Postfach übermittelt und dort gespeichert, mithin empfangen wurde. Die Zugangsfiktion dient dem Schutz der nicht professionellen Verfahrensbeteiligten und soll zugleich einen Anreiz für den elektronischen Übermittlungsweg setzen. Der Nachweis eines fehlenden oder späteren Zugangs bleibt nach Satz 5 möglich.[360]

Diese Vorschrift beschreibt funktional die Bereitstellungsbestätigung nach ADR-0018, verlangt für sie aber ebenfalls kein qualifiziertes Element. Von ihr zu unterscheiden ist der Nachweis der Zustellung an berufsmäßig Beteiligte nach § 173 Abs. 3 ZPO, der ein aktiv abzugebendes elektronisches Empfangsbekenntnis als strukturierten Datensatz verlangt und in der Zielarchitektur über die Lesebestätigung abzubilden wäre (ADR-1118).

[359] Siebert, in: Saenger, 10. Aufl. 2023, ZPO, § 173, Rn. 5.
[360] Siebert, in: Saenger, 10. Aufl. 2023, ZPO, § 173, Rn. 5.

2.1.3. Keine ergänzenden Vorgaben in der ERVV

Die ERVV enthält zur Sicherung von Quittungen keine Regelungen. Ihre technischen Anforderungen betreffen nach § 2 und § 5 ERVV Dateiformate, Höchstgrenzen und strukturierte Datensätze, nach § 4 ERVV die Übermittlungswege für qualifiziert signierte Dokumente und nach §§ 10 bis 13 ERVV die Anforderungen an die Postfächer. Die Nachweisebene regelt sie nicht.

Für den elektronischen Rechtsverkehr gilt damit in beiden Richtungen, dass ein fortgeschrittenes Siegel dem gesetzlichen Anforderungsprofil genügt. Qualifizierte Zeitstempel oder qualifizierte Siegel sind für den Zugangsnachweis (siehe zum Begriff die Vorbemerkung zu 2) nicht vorgeschrieben.

2.1.4. Beweiskraft im Rahmen freier Beweiswürdigung

Nichtqualifizierte Nachweise sind zulässig, aber nicht gleichwertig. Nichtqualifizierte wie qualifizierte Nachweise sind gleichermaßen als Beweismittel zulässig (vgl. Art. 35 Abs. 1, Art. 41 Abs. 1 und Art. 43 Abs. 1 eIDAS-VO). Elektronische Dokumente werden dabei nach § 371 Abs. 1 Satz 2 ZPO als Augenscheinsobjekte in den Prozess eingebracht. Für elektronische Siegel und Zeitstempel gilt nichts anderes.[361] Ihr Beweiswert unterliegt dann der freien Beweiswürdigung nach § 286 Abs. 1 ZPO.[362]

Der Beweiswert eines lediglich fortgeschritten gesicherten Nachweises ist damit nicht wertlos, aber angreifbar. Gegenüber ungesicherten Dokumenten ist der Beweiswert erhöht. Soweit keine spezifische Beweiserleichterung eingreift (dazu sogleich), bedarf es aber im Regelfall einer ergänzenden Beweisaufnahme durch Sachverständigengutachten.[363] Hierdurch entsteht ggf. gegenüber qualifiziert gesicherten Dokumenten aus prozessökonomischer Sicht ein Mehraufwand.

[361] Lapp, in: BeckOK IT-Recht, 22. Ed. 1.4.2025, Art. 35 VO (EU) 910/2014, Rn. 8 und Art. 41 VO (EU) 910/2014, Rn. 5 f.
[362] Pickenpack, in: BeckOK IT-Recht, 22. Ed. 1.10.2025, § 371a ZPO, Rn. 1.
[363] Roßnagel, in: Hornung/Schallbruch, IT-SicherheitsR, § 14, Rn. 91.

2.2. Die Bereitstellungsbestätigung nach ADR-0018 als Zugangsnachweis

Vor der Betrachtung von Möglichkeiten zur Aufwertung des Beweiswerts durch qualifizierte Elemente ist zu bestimmen, was die in ADR-0018 vorgesehene Bestätigung nach geltendem Recht aus sich heraus leistet. Sie besteht aus vier Elementen: dem Eingangszeitpunkt im Machtbereich des Empfängers, einem kryptografischen Hash über das Chiffrat der Nachricht, einer Referenz auf die Originalnachricht sowie einer Signatur des empfangenden Servers, deren öffentlicher Schlüssel im Self-Service-Portal hinterlegt ist. Hinzu tritt die adressierte MXID des Empfängers.

2.2.1. Der jeweils geschuldete Beweis

Welchen Beweis die Bestätigung erbringen muss, unterscheidet sich je nach Regime, und zwar in einer für ZaPuK günstigen Weise. Bei den Abrufmodellen verlangt das Gesetz von der Behörde nur den Nachweis der Bereitstellung: nach § 9 Abs. 1 Satz 5 OZG „die Bereitstellung und den Zeitpunkt der Bereitstellung", nach § 122a Abs. 4 Satz 2 AO „den Zeitpunkt der Bereitstellung zum Abruf". Weitergehend ist § 41 Abs. 2 Satz 3 VwVfG bei der elektronischen Übermittlung, wo die Behörde im Zweifel „den Zugang des Verwaltungsaktes und den Zeitpunkt des Zugangs" nachzuweisen hat. Noch anders ist es schließlich nach § 37 Abs. 2a Satz 5 SGB X, wonach die Behörde „den Zugang der Benachrichtigung" (über die Bereitstellung zum Abruf) nachweisen muss. Schließlich kommt es bei der Bekanntgabe eines Verwaltungsakts durch Abruf über öffentliche Netze auf den tatsächlichen Abruf an (und somit auf den Beweis von dessen Zeitpunkt), damit am Folgetag die Bekanntgabefiktion eintritt (§ 41 Abs. 2a Satz 3 VwVfG). § 173 Abs. 4 Satz 4 ZPO, der sich auf die Zustellung über einen sicheren Übermittlungsweg bezieht, stellt auf den „ausgewiesenen Tag des Eingangs in dem vom Empfänger eröffneten elektronischen Postfach" ab, welcher somit zu nachzuweisen ist.

Die Bereitstellungsbestätigung belegt den Eingang des Chiffrats im Postfach des Empfängers. Sie deckt damit die Anforderungen des § 41 Abs. 2 Satz 3 VwVfG und des § 173 Abs. 4 Satz 4 ZPO unmittelbar ab und geht über das hinaus, was § 9 OZG und § 122a AO verlangen – dort genügt bereits der frühere und behördenseitig kontrollierbare Vorgang der Bereitstellung. Für die Abrufmodelle ist die Bestätigung folglich ein Nachweis mit Sicherheitsmarge. Ihre

eigentliche Bedeutung entfaltet sie in den Übermittlungsmodellen und im elektronischen Rechtsverkehr.

2.2.2. Wirkung der einzelnen Nachweiselemente

Der Eingangszeitpunkt ist das für die Fristberechnung entscheidende Element. Er beruht auf der Systemzeit des empfangenden Backends und nicht auf einer an die koordinierte Weltzeit gebundenen, gegen unbemerkte Veränderung gesicherten Zeitquelle. Eine Vermutung der Richtigkeit besteht daher nicht. Das Gericht würdigt ihn nach § 286 Abs. 1 ZPO frei. In der freien Würdigung fällt allerdings erheblich ins Gewicht, dass die Zeitangabe nicht vom beweisbelasteten Absender stammt (dazu sogleich).

Der Hash über das Chiffrat bindet die Bestätigung an genau diejenige Nachricht, um die gestritten wird. Er entkräftet den Einwand, es sei zwar eine, aber nicht diese Nachricht eingegangen. Über den Inhalt sagt er (unmittelbar) nichts aus, weil er nicht am Klartext gebildet wird – das ist die notwendige Kehrseite der Ende-zu-Ende-Verschlüsselung und entspricht dem Muster der Prüfsumme nach § 5 Abs. 8 und 9 De-Mail-G. Praktisch bedeutsam ist insofern, dass der Hash für den Absender nur dann verwertbar ist, wenn er das übermittelte Chiffrat – oder die zu seiner Reproduktion nötigen Parameter – aufbewahrt hat. Wer allein den Klartext archiviert, kann im Streitfall nicht zeigen, dass sich der bestätigte Hash auf sein Dokument bezieht.

Die Referenz auf die Originalnachricht ordnet die Bestätigung dem Vorgang zu. Für sich genommen hat sie als systeminterne Kennung geringes Gewicht. Ihre Aussagekraft ergibt sich erst im Zusammenhang mit dem Vorgangsraum und dem Exportpaket.

Die Signatur des empfangenden Servers trägt die Aussage über die Herkunft. Ihr Beweiswert hängt davon ab, ob sich der verwendete Schlüssel einem bestimmten Betreiber zurechnen lässt und ob diese Zurechnung auch nachträglich noch nachvollziehbar ist. Beides leistet die Hinterlegung im Self-Service-Portal nur, wenn die Registrierung dokumentiert und die Schlüsselhistorie vorgehalten wird (ADR-1144). Ohne Zertifikatsbindung an eine juristische Person handelt es sich um eine bloße Serverschlüsselbindung, deren Zuordnung im Bestreitensfall gesondert dargelegt werden müsste.

2.2.3. Die Rollenverteilung als beweiswerterhöhendes Element

Der Umstand, dass die Bestätigung nicht vom Absender, sondern vom Backend der Empfängerseite erzeugt wird, sollte im Rahmen freier Beweiswürdigung erheblich vertrauensbildend wirken. Die beweisbelastete Behörde legt damit keine selbst erstellte Aufzeichnung vor, sondern die Erklärung einer dritten Stelle über einen Vorgang in deren eigenem Machtbereich (wobei es sich bei einem zentral betriebenen Backend bei der dritten Stelle ebenfalls um eine staatliche Stelle handelt). Im Rahmen der freien Beweiswürdigung ist das gegebenenfalls ein erheblicher Unterschied gegenüber einem behördlichen Versandprotokoll, das der Gegenseite regelmäßig als Aufzeichnung in eigener Sache entgegengehalten wird.

Dieser Vorteil steht und fällt mit der organisatorischen Trennung von Absender und Backend-Betreiber. Für die Architektur spricht dies dafür, die Betreibertrennung nicht nur unter dem Gesichtspunkt des Metadatenschutzes zu betrachten, sondern auch als ggf. beweisrechtlich werthaltige Eigenschaft.

2.2.4. Grenzen und Einführung in den Prozess

Die Bestätigung belegt den Eingang des Chiffrats, nicht dessen Entschlüsselbarkeit, nicht die Kenntnisnahme und nicht den Inhalt. Zur Entschlüsselbarkeit und ihrer Bedeutung für die Tragfähigkeit der Zugangsfiktionen wird auf III.3.6.2 verwiesen; die Kenntnisnahme ist Gegenstand der Abruf- und Lesebestätigungen (ADR-1118), der Inhalt Gegenstand des qualifizierten Siegels (ADR-0017).

Für die Einführung in den Prozess gilt § 371 Abs. 1 Satz 2 ZPO. Der Beweis wird durch Vorlegung oder Übermittlung der Datei angetreten. Maßgeblich ist das signierte Originalereignis. Nur an ihm lassen sich Integrität und Authentizität durch einen Sachverständigen prüfen.[364] Ein Bildschirmfoto oder eine gerenderte Darstellung ist zwar als elektronisches Dokument zulässig – der BGH hat einen Screenshot einer beA-Störungsmeldung als solches eingeordnet –,[365] verliert

[364] Pickenpack, in: BeckOK IT-Recht, 22. Ed. 1.10.2025, § 371 ZPO, Rn. 12.
[365] BGH, NJW 2023, 3799.

aber gerade die kryptografische Prüfbarkeit. Die Bestätigung muss deshalb in maschinell prüfbarer Originalform exportierbar sein.

2.3. Beweiserleichterungen/Vermutungen

Bei Einhaltung einer vorgeschriebenen Form (2.3.1) oder Nutzung qualifizierter Verfahren nach eIDAS (2.3.2, 2.3.3 und 2.3.4) greifen prozessual die folgenden Beweiserleichterungen bzw. Vermutungsregeln ein.

2.3.1. Öffentliche elektronische Dokumente – Beweiskraft öffentlicher Urkunden

Die Beweiskraft öffentlicher elektronischer Dokumente (als Urkunden) ist deutlich erhöht. Nach § 371a Abs. 3 Satz 1 ZPO finden auf elektronische Dokumente, die eine öffentliche Behörde innerhalb der Grenzen ihrer Amtsbefugnisse in der vorgeschriebenen Form erstellt hat, die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Diese Beweiskraft kommt öffentlichen elektronischen Dokumenten ausdrücklich auch ohne qualifizierte elektronische Signatur zu.[366] Sie ist erheblich: Über den Verweis auf §§ 415, 417 und 418 ZPO wird voller Beweis sowohl darüber erbracht, dass die Erklärung vom Ersteller herrührt, als auch über den beurkundeten Vorgang selbst. Dem Gegner bleibt nur der Beweis des Gegenteils nach § 415 Abs. 2 ZPO, und zwar beschränkt auf formelle Faktoren.[367]

Für ZaPuK ist dies praktisch bedeutsam. Eine Bereitstellungsbestätigung ist der Sache nach eine Zeugnisurkunde über den Eingangszeitpunkt. Erfüllt sie die Voraussetzungen des § 371a Abs. 3 Satz 1 ZPO, erbringt sie über § 418 Abs. 1 ZPO vollen Beweis der bezeugten Tatsache – also desjenigen Umstands, den die Behörde nach § 9 Abs. 1 Satz 5 OZG und § 122a Abs. 4 Satz 2 AO im Zweifel nachzuweisen hat. Der Gegenbeweis der Unrichtigkeit bleibt nach § 418 Abs. 2 ZPO zulässig, ist aber ungleich schwerer zu führen als die Erschütterung einer frei zu würdigenden Aufzeichnung.

[366] Pickenpack, in: BeckOK IT-Recht, 22. Ed. 1.10.2025, § 371a ZPO, Rn. 23.
[367] Pickenpack, in: BeckOK IT-Recht, 22. Ed. 1.10.2025, § 371a ZPO, Rn. 21.

Einschränkend ist zu beachten, dass die Vorschrift nur für behördlich betriebene Backends greift. Für Bestätigungen privat betriebener souveräner Backends bleibt es bei § 371a Abs. 1 ZPO. Zudem verlangt Satz 1 die Erstellung „in der vorgeschriebenen Form". Daran könnte es fehlen, weil keine Rechtsvorschrift die Form der Bereitstellungsbestätigung festlegt. Hieraus folgt die unten formulierte Empfehlung einer verordnungsrechtlichen Formvorgabe.

2.3.2. Öffentliche elektronische Dokumente – Echtheitsvermutung bei QES

Ist das Dokument mit einer qualifizierten elektronischen Signatur oder – seit der Änderung durch Gesetz vom 8. Dezember 2025 – einem qualifizierten elektronischen Siegel versehen, tritt nach § 371a Abs. 3 Satz 2 ZPO die Vermutung der Echtheit nach § 437 ZPO hinzu. Der zuvor geführte Streit, ob ein qualifiziertes Siegel hierfür genügt, hat sich damit erledigt. Er wurde bis dahin unter Hinweis darauf verneint, dass die eIDAS-VO zwischen Siegel und Signatur unterscheidet und das Siegel nicht im selben Maße Gewähr für die Authentizität biete.[368] Für eine serverseitig erzeugte Quittung ist das eine entscheidende Klarstellung, weil ein Siegel – anders als eine Signatur – einer juristischen Person zugeordnet werden kann.

Im Vergleich zu privaten elektronischen Dokumenten ergibt sich eine Asymmetrie. Für diese verweist § 371a Abs. 1 Satz 1 ZPO ausschließlich auf die qualifizierte elektronische Signatur und die notariell beglaubigte elektronische Unterschrift. Ein qualifiziertes Siegel eröffnet dort die Privaturkunden-Beweiskraft nach § 416 ZPO nicht. Souveräne Backends privater Organisationen können diese Stufe folglich nach geltender Rechtslage über ein Siegel formal nicht erreichen.

2.3.3. Qualifizierte elektronische Zeitstempel – Vermutung der Richtigkeit

Für qualifizierte elektronische Zeitstempel gilt nach Art. 41 Abs. 2 eIDAS-VO die Vermutung der Richtigkeit des angegebenen Datums und der Zeit sowie der Unversehrtheit der damit verbundenen Daten. Sie deckt damit dasjenige Element ab, an das die Fiktionen des § 173 Abs. 4

[368] Pickenpack, in: BeckOK IT-Recht, 22. Ed. 1.10.2025, § 371a ZPO, Rn. 25.

Satz 4 ZPO, des § 9 Abs. 1 Satz 4 OZG und des § 122a Abs. 4 AO anknüpfen. Der in ADR-0018 vorgesehene einfache Zeitstempel begründet diese Vermutung nicht.

2.3.4. Qualifizierter Zustelldienst – Vermutungen gem. Art. 43 Abs. 2 eIDAS-VO

Schließlich führt die Nutzung eines qualifizierten Zustelldienstes zu der Zustellvermutung nach Art. 43 Abs. 2 eIDAS-VO. Sie wurde im Zusammenhang mit der beweissicheren Übermittlung bereits dargestellt und erfordert nach Art. 44 Abs. 1 eIDAS-VO neben der Erbringung durch einen qualifizierten Vertrauensdiensteanbieter und der Identifizierung beider Seiten auch qualifizierte Zeitstempel für Absenden und Empfangen (vgl. 2.1.4 sowie unten VII.1.3).

Zur Reichweite dieser Vermutungen besteht Streit. Nach einer Auffassung handelt es sich um gesetzliche Vermutungen im Sinne des § 292 ZPO, die nur durch den vollen Beweis des Gegenteils entkräftet werden können und damit deutlich über den Anscheinsbeweis des § 371a Abs. 1 Satz 2 ZPO hinausgehen.[369] Nach der Gegenauffassung scheidet diese Lesart aus, weil die eIDAS-VO die Rechtswirkungen der Vermutung ausdrücklich nicht geregelt und deren Bestimmung damit den Mitgliedstaaten überlassen hat; zudem wäre es wertungswidersprüchlich, dem Siegel eine stärkere Wirkung beizulegen als der qualifizierten Signatur, obwohl das Missbrauchsrisiko beim Siegel höher ist, weil es sicherheitstechnisch nicht an eine Person gebunden ist.[370] Für die hier zu treffende Empfehlung kann der Streit offenbleiben. Auch bei der engeren Lesart bleibt die Beweiserleichterung gegenüber der freien Würdigung eines bloß fortgeschritten gesicherten Nachweises erheblich.

2.4. Trennung von Siegelniveau und Anbieterstatus

Hervorzuheben ist, dass das für die Zeitvermutung maßgebliche Merkmal nicht die Qualifiziertheit des Siegels ist, sondern der Status des Ausstellers. Nach Art. 42 Abs. 1 Buchstabe c eIDAS-VO wird der qualifizierte Zeitstempel mit einer fortgeschrittenen Signatur unterzeichnet oder einem fortgeschrittenen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt.

[369] Lapp, in: BeckOK IT-Recht, 22. Ed. 1.4.2025, Art. 35 VO (EU) 910/2014, Rn. 15 und Art. 41 VO (EU) 910/2014, Rn. 7.
[370] Roßnagel, in: Hornung/Schallbruch, IT-SicherheitsR, 2. Aufl. 2025, § 14, Rn. 98, 100.

Hinzu treten die Bindung an eine mit der koordinierten Weltzeit verknüpfte Zeitquelle und der Ausschluss unbemerkter Veränderung.

Diese Konstruktion ist im deutschen elektronischen Rechtsverkehr bereits erprobt. Der Transfervermerk nach § 298 Abs. 3 ZPO muss Angaben zum Zeitpunkt der Signaturanbringung enthalten, und weil dieser Zeitpunkt nicht vom Absender beeinflussbar sein darf, ist er als qualifizierter elektronischer Zeitstempel im Sinne des Art. 42 eIDAS-VO anzubringen – versehen mit einer fortgeschrittenen Signatur oder einem fortgeschrittenen Siegel eines qualifizierten Vertrauensdiensteanbieters, technisch umgesetzt über eine Timestamping Authority nach RFC 3161.[371] Was für den Transfervermerk gilt, lässt sich auf die Bereitstellungsbestätigung übertragen.

Daraus folgt, dass der qualifizierte Zeitstempel ein von außen beziehbarer Dienst ist. Ein Postfach-Backend kann den Zeitstempel eines qualifizierten Anbieters in seine – im Übrigen fortgeschritten gesiegelte – Bereitstellungsbestätigung einbinden, ohne selbst qualifizierter Vertrauensdiensteanbieter zu werden. Dies löst das in ADR-1145 beschriebene Skalierungsproblem für den souveränen Betrieb weitgehend auf: Der aufwendige Statuserwerb ist auf einen zentralen Zeitstempeldienst zu bündeln, nicht auf jedes einzelne Backend.

Zu prüfen bleibt ferner, ob die in ADR-0018 vorgesehene Ed25519-Serversignatur überhaupt ein elektronisches Siegel im Sinne der eIDAS-VO darstellt. Ein Siegel setzt nach Art. 3 Nr. 24 und 25 eIDAS-VO einen Siegelersteller voraus, der eine juristische Person ist, und ein fortgeschrittenes Siegel verlangt nach Art. 36 eIDAS-VO die eindeutige Zuordnung zu diesem Siegelersteller, dessen Identifizierbarkeit, die alleinige Kontrolle über die Siegelerstellungsdaten und die Erkennbarkeit nachträglicher Veränderungen. Das Rechtsinstitut des elektronischen Siegels wurde gerade zu dem Zweck geschaffen, den Personenbezug der Signatur durch einen Organisationsbezug abzulösen.[372] Für eine maschinell erzeugte Serverquittung ist es damit die passende Form. Eine bloße, im Self-Service-Portal hinterlegte Serverschlüsselbindung dürfte

[371] Loos, in: BeckOK IT-Recht, 22. Ed. 1.4.2025, § 130a ZPO, Rn. 49.
[372] Lapp, in: BeckOK IT-Recht, 22. Ed. 1.4.2025, Art. 35 VO (EU) 910/2014, Rn. 3.

den Anforderungen des Art. 36 eIDAS-VO jedoch nicht genügen; erforderlich ist eine Zertifikatsbindung an den Betreiber als juristische Person.

2.5. Folgerungen für die Architektur von ZaPuK

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Im Hinblick auf den ERV mit Gerichten sind die beiden Übermittlungsrichtungen auseinanderzuhalten. Die Bereitstellungsbestätigung nach ADR-0018 ist das Gegenstück zur empfängerseitigen Eingangsbestätigung des § 173 Abs. 4 Satz 4 ZPO. Die gerichtsseitige Eingangsbestätigung nach § 130a Abs. 5 Satz 2 ZPO erzeugt ZaPuK dagegen nicht. Sie ist über den Protokollkonverter (ADR-0010) aus der EGVP-Infrastruktur entgegenzunehmen, dem Absender anzuzeigen und mit dem Vorgang zu speichern. Da die anwaltliche Sorgfalt die Kontrolle von Meldetext und Übermittlungsstatus verlangt, muss der Postfachzugang diese Angaben unverfälscht darstellen und in das Exportpaket nach ADR-1135 übernehmen.

- Die Bereitstellungsbestätigung in ihrer bisherigen Ausgestaltung trägt den jeweils geschuldeten Nachweis. Sie deckt § 41 Abs. 2 Satz 3 VwVfG und § 173 Abs. 4 Satz 4 ZPO unmittelbar ab und geht über die Anforderungen der Abrufmodelle (§ 9 Abs. 1 Satz 5 OZG, § 122a Abs. 4 Satz 2 AO) hinaus. Die Grundentscheidung des ADR-0018 wird insoweit bestätigt. Eine Pflicht zur Nachrüstung qualifizierter Elemente besteht nach geltendem Recht nicht.

- Der beweisrechtliche Vorteil der Bestätigung beruht wesentlich darauf, dass sie nicht vom beweisbelasteten Absender, sondern vom Backend der Empfängerseite erzeugt wird. Die organisatorische Trennung der Backend-Betreiber sollte deshalb auch unter diesem Gesichtspunkt aufrechterhalten werden; wo Absender und Backend-Betreiber zusammenfallen, entfällt der Vorteil.

- Der Ciphertext-Hash ist für den Absender nur verwertbar, wenn er das übermittelte Chiffrat oder die zu seiner Reproduktion nötigen Parameter aufbewahrt. Das

Exportpaket nach ADR-1135 sollte dies ausdrücklich aufnehmen; die Aufbewahrung allein des Klartextes genügt nicht.

- Die Bestätigung muss in maschinell prüfbarer Originalform exportierbar sein, weil der Beweis nach § 371 Abs. 1 Satz 2 ZPO durch Vorlegung oder Übermittlung der Datei angetreten wird und nur am Original eine sachverständige Prüfung möglich ist. Eine gerenderte Darstellung oder ein Bildschirmfoto genügt hierfür nicht.

- Die Serversignatur sollte als fortgeschrittenes Siegel nach Art. 36 eIDAS-VO ausgestaltet werden, also mit Zertifikatsbindung an den Betreiber als juristische Person und gesicherter alleiniger Kontrolle über die Siegelerstellungsdaten. Dies ist in ADR-1144 zu verankern und über die Anschlussbedingungen (ADR-1145) verbindlich zu machen.

- Ein qualifizierter elektronischer Zeitstempel würde nach Art. 41 Abs. 2 eIDAS-VO das Element absichern, an das die Zugangs- und Bekanntgabefiktionen anknüpfen und für das die Behörde die Beweislast trägt. Er sollte über einen zentralen, von einem qualifizierten Vertrauensdiensteanbieter erbrachten Zeitstempeldienst bezogen und allen Backends – auch den souverän betriebenen – bereitgestellt werden. Die Konstruktion entspricht derjenigen des Transfervermerks nach § 298 Abs. 3 ZPO.

- Es wird empfohlen, die Form der Bereitstellungsbestätigung durch Rechtsvorschrift festzulegen – in Betracht kommen eine Regelung nach § 5 oder § 6 OZG, die Verordnung nach § 3c Abs. 2 VwVfG n.F. oder eine spezialgesetzliche Grundlage. Damit wäre das Tatbestandsmerkmal „in der vorgeschriebenen Form erstellt“ des § 371a Abs. 3 Satz 1 ZPO erfüllt und der Weg zur Urkundenbeweiskraft nach §§ 415, 417, 418 ZPO eröffnet.

- Ein qualifiziertes Siegel ist dort zu erwägen, wo zusätzlich die Echtheitsvermutung des § 371a Abs. 3 Satz 2 ZPO in Verbindung mit § 437 ZPO angestrebt wird. Der frühere Streit, ob ein Siegel hierfür genügt, ist durch die Neufassung der Vorschrift zugunsten des Siegels entschieden.

- Zu berücksichtigen ist die Asymmetrie zwischen öffentlichen und privaten Backends. Bestätigungen behördlich betriebener Backends können über § 371a Abs. 3 ZPO die Beweiskraft öffentlicher Urkunden erlangen. Bestätigungen privat betriebener souveräner Backends unterfallen § 371a Abs. 1 ZPO, der das Siegel nicht kennt. Für diese Backends bleibt es bei der freien Beweiswürdigung, sofern nicht der Weg über einen qualifizierten Zustelldienst gewählt wird.

- Das Sicherungsniveau muss nicht einheitlich sein. Es lässt sich über die absendergesteuerten Zustelloptionen (ADR-1119) abstufen, sodass qualifizierte Zeitstempel nur dort erzeugt werden, wo der Anwendungsfall sie erfordert. Das entspricht zugleich dem Grundsatz der Datenminimierung, weil jeder zusätzliche Nachweis weitere unverschlüsselte Metadaten erzeugt.

- Die Langzeitprüfbarkeit ist mitzuplanen. Zeitstempel und Siegel müssen auch nach Ablauf der Zertifikatsgültigkeit prüfbar bleiben; Statushistorien und Prüfschlüssel sind über den Aufbewahrungszeitraum vorzuhalten (ADR-1144). Dies deckt sich mit der Anforderung, die Gültigkeit stets bezogen auf den Versandzeitpunkt und nicht auf den Prüfzeitpunkt beurteilen zu können.

- Gegenüber den Teilnehmern ist Transparenz herzustellen. Für Backends, deren Bestätigungen nur fortgeschritten gesichert sind, sollte erkennbar gemacht werden, dass sie lediglich die Wirkung des Art. 43 Abs. 1 eIDAS-VO entfalten und im Bestreitensfall Sachverständigenbeweis erfordern können.

3. Formwirksame Einreichung im elektronischen Rechtsverkehr – ZaPuK als sicherer Übermittlungsweg

Kurzzusammenfassung. Eine qualifizierte elektronische Signatur auf dem einzelnen Dokument ist für den elektronischen Rechtsverkehr nicht zwingend. § 130a Abs. 3 Satz 1 ZPO stellt zwei gleichrangige Wege zur Verfügung: die qualifizierte elektronische Signatur der verantwortenden Person oder deren einfache Signatur in Verbindung mit der Einreichung auf einem sicheren

Übermittlungsweg. ZaPuK kann daher – wie das besondere elektronische Bürger- und Organisationenpostfach (eBO) – als sicherer Übermittlungsweg die Formwirksamkeit tragen.

Der für ZaPuK einschlägige Anknüpfungspunkt ist der Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Abs. 5 OZG (§ 130a Abs. 4 Satz 1 Nr. 4 ZPO in Verbindung mit § 13 ERVV). Auf dieser Grundlage beruht bereits das heutige „Mein Justizpostfach" (MJP). Die Anforderungen an die Bindung von Absenderidentität und Postfach ergeben sich abschließend aus § 13 Abs. 1 ERVV: ein dem Stand der Technik entsprechender Protokollstandard, eine Identitätsfeststellung mit einem der dort abschließend genannten Mittel, eine Authentisierung beim Versand und die Feststellbarkeit, dass das Dokument vom Nutzer des Postfach- und Versanddienstes versandt wurde. Letzteres ist der vertrauenswürdige Herkunftsnachweis. Er muss aus einem Prüf- oder Transfervermerk hervorgehen und lässt sich dem Dokument selbst gerade nicht entnehmen.

Für die Architektur bedeutet dies: (1) Die pseudonyme Adressierung (ADR-1104, ADR-1105) steht der Anerkennung nicht entgegen, weil die Identitätsfeststellung nicht an der Adresse, sondern am Identifizierungsmittel ansetzt. (2) Die einfache Signatur der verantwortenden Person im Dokument bleibt zwingend und ist im Postfachzugang zu erzwingen oder wenigstens anzumahnen. (3) Am Übergabepunkt zur Justiz ist ein dem vertrauenswürdigen Herkunftsnachweis entsprechendes, maschinell prüfbares Artefakt zu erzeugen oder durchzureichen (ADR-0010). Dies ist von der Bereitstellungsbestätigung (ADR-0018) zu unterscheiden. (4) Die Bindung an das OZG-Nutzerkonto ist ein Abhängigkeitsrisiko: Wird die Kopplung von Postfach und Nutzerkonto (§ 2 Abs. 7 Satz 2 OZG) im Zuge der empfohlenen OZG-Anpassung gelöst, entfällt zugleich der Anknüpfungspunkt des § 130a Abs. 4 Satz 1 Nr. 4 ZPO und seiner Parallelvorschriften.

3.1. Der Regelungsrahmen: zwei gleichrangige Wege

Nach § 130a Abs. 3 Satz 1 ZPO muss das elektronische Dokument mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden. Der BGH

beschreibt dies als zwei nebeneinanderstehende Wege zur rechtswirksamen Übermittlung.[373] Das Bundesverwaltungsgericht hebt den „systematische[n] Gleichrang beider Tatbestandsalternativen" hervor und leitet daraus zugleich ab, dass das Erfordernis des sicheren Übermittlungswegs so zu konkretisieren ist, dass es zuverlässigen Schutz vor nicht autorisierten Versendungen und Textmanipulationen bietet.[374]

Das Adjektiv „sicher" bezieht sich dabei nicht auf IT-Sicherheit oder Ausfallschutz, sondern darauf, dass ein sicherer Rückschluss auf die Identität des Absenders möglich ist. Der Kommunikationskanal ersetzt die Identifikationsfunktion der Unterschrift.[375] Deshalb kann auf die qualifizierte Signatur verzichtet werden.

Die Parallelvorschriften der übrigen Verfahrensordnungen sind wortgleich gefasst: § 55a Abs. 3 und 4 VwGO, § 46c Arbeitsgerichtsgesetz (ArbGG), § 65a Sozialgerichtsgesetz (SGG), § 52a Finanzgerichtsordnung (FGO) sowie § 32a Strafprozessordnung (StPO). Die technischen Rahmenbedingungen regelt für alle diese Verfahren einheitlich die Elektronischer-Rechtsverkehr-Verordnung (§ 1 Abs. 1 ERVV). Die nachfolgenden Ausführungen gelten daher verfahrensübergreifend.

3.2. Der einschlägige Übermittlungsweg für ZaPuK

Der Katalog des § 130a Abs. 4 Satz 1 ZPO nennt in der geltenden Fassung fünf Wege: den Übermittlungsweg zwischen den besonderen elektronischen Anwaltspostfächern nach §§ 31a, 31b BRAO oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (Nr. 1), den Weg über ein nach Durchführung eines Identifizierungsverfahrens eingerichtetes Postfach einer Behörde oder einer juristischen Person des öffentlichen Rechts (Nr. 2), den Weg über ein nach Durchführung eines Identifizierungsverfahrens eingerichtetes elektronisches Postfach einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung (Nr. 3), den Weg über einen nach Durchführung eines Identifizierungsverfahrens genutzten Postfach- und Versanddienst eines

[373] BGH, Beschluss vom 11.03.2025 – VI ZB 5/24, Rn. 6.
[374] BVerwG, Beschluss vom 12.10.2021 – 8 C 4/21, Rn. 5.
[375] Müller, in: Hornung/Schallbruch IT-SicherheitsR, § 27, Rn. 98.

Nutzerkontos im Sinne des § 2 Abs. 5 OZG (Nr. 4) und schließlich sonstige bundeseinheitliche Übermittlungswege, die durch Rechtsverordnung festgelegt werden (Nr. 5).

Für ZaPuK ist Nr. 4 der tragende Anknüpfungspunkt. Auf ihm beruht bereits „Mein Justizpostfach", das die Rechtsprechung ohne Weiteres als sicheren Übermittlungsweg behandelt (OLG Hamm, Beschl. v. 1.7.2024 – 22 U 15/24). Da ZaPuK das MJP ablösen soll, ist der Anschluss strukturell vorgezeichnet und bedarf keiner neuen gesetzlichen Kategorie.

Die teilnehmergruppenbezogene Aufteilung der Postfach-Backends (ADR-1103) lässt sich dabei auf den Katalog abbilden. Privatpersonen und private Organisationen können über Nr. 4 angebunden werden, weil das Nutzerkonto nach § 2 Abs. 5 Sätze 3 und 4 OZG sowohl als Bürger- wie als Organisationskonto bereitgestellt wird; öffentliche Stellen ebenfalls über Nr. 4, da das Organisationskonto ausdrücklich auch Behörden zur Verfügung steht (vgl. § 3 Abs. 3 OZG), alternativ über Nr. 2 als besonderes elektronisches Behördenpostfach nach §§ 6 bis 9 ERVV. Für private Organisationen bleibt daneben der eBO-Weg nach Nr. 3 in Verbindung mit §§ 10 bis 12 ERVV offen.

Der Weg über Nr. 4 ist gegenüber dem eBO-Weg deutlich schlanker. § 10 Abs. 1 Nr. 3 ERVV verlangt für das eBO zwingend die Eintragung des Postfachinhabers in ein sicheres elektronisches Verzeichnis, und § 11 Abs. 1 ERVV schaltet eine von den Ländern zu bestimmende öffentlich-rechtliche Stelle vor, die die Freischaltung veranlasst. § 13 Abs. 3 Satz 1 ERVV fordert die Verzeichniseintragung demgegenüber nur, „soweit dies zum Betrieb des jeweiligen Postfach- und Versanddienstes erforderlich ist". Das ist für ZaPuK erheblich: Die Grundentscheidung, für Privatpersonen kein Adressregister zu führen (ADR-1111), lässt sich unter Nr. 4 wahren, während sie unter Nr. 3 an § 10 Abs. 1 Nr. 3 ERVV scheitern würde. Hinzu kommt, dass § 13a Abs. 1 Nr. 1 ERVV für natürliche Personen im Verzeichnis Vor- und Nachname sowie Anschrift vorsieht – eine Angabe, die mit der bereichsspezifischen pseudonymen Adressierung nach ADR-1105 nicht vereinbar wäre.

3.3. Die Bindung von Absenderidentität und Postfach

Welche Anforderungen die Bindung erfüllen muss, ergibt sich abschließend aus § 13 Abs. 1 ERVV. Die vier dort genannten Voraussetzungen müssen kumulativ vorliegen.

3.3.1. Protokollstandard

Erforderlich ist eine technische Vorrichtung, die „auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht" (§ 13 Abs. 1 Nr. 1 ERVV). Die Norm ist bewusst protokolloffen formuliert. Das Matrix-Protokoll (ADR-0011) ist darunter subsumierbar. Problematisch ist das Fehlen eines Feststellungs- oder Zulassungsverfahrens: Die ERVV kennt keinen Mechanismus, mit dem verbindlich festgestellt würde, dass ein bestimmter Protokollstandard OSCI im Sinne der Vorschrift ersetzt. Ohne Klarstellung besteht Rechtsunsicherheit und jedes Gericht müsste die Frage inzident prüfen.

3.3.2. Feststellung der Identität

Die Identität des Nutzers muss durch ein Identifizierungsmittel nach § 11 Abs. 2 Satz 2 Nr. 1 oder 2 ERVV oder durch ein nach § 87a Abs. 6 AO in der Steuerverwaltung eingesetztes sicheres Verfahren festgestellt sein (§ 13 Abs. 1 Nr. 2 ERVV). Zulässig sind damit ausschließlich der elektronische Identitätsnachweis nach § 18 PAuswG, § 12 eIDKG oder § 78 Abs. 5 AufenthG, ein qualifiziertes elektronisches Siegel nach Art. 38 eIDAS-VO sowie das ELSTER-Verfahren.

Daraus folgt Konkretes für die Authentisierungsentscheidungen der Zielarchitektur (ADR-0014 bis ADR-0016). BundID trägt, soweit die Anmeldung über die eID-Funktion erfolgt; das ELSTER-Organisationszertifikat des Unternehmenskontos trägt über die Variante des § 87a Abs. 6 AO. Eine Anmeldung mit BundID auf niedrigem Vertrauensniveau – Benutzername und Passwort – genügt dagegen nicht. Ebenso wenig ist die EUDI-Wallet im Katalog genannt. Sie ist derzeit kein zulässiges Identifizierungsmittel im Sinne des § 11 Abs. 2 Satz 2 ERVV. Die Architektur muss folglich das Identifizierungsniveau je Postfach nachhalten und für die ERV-Nutzung exponieren, und für die Wallet-Anbindung (ADR-0014, perspektivisch EU Business Wallet) besteht Ergänzungsbedarf auf Verordnungsebene.

3.3.3. Authentisierung beim Versand

Der Nutzer muss sich beim Versand eines elektronischen Dokuments entsprechend § 11 Abs. 3 ERVV authentisieren (§ 13 Abs. 1 Nr. 3 ERVV). Zulässig sind der elektronische Identitätsnachweis, ein Authentisierungszertifikat auf einer qualifizierten elektronischen Signaturerstellungseinheit nach Anhang II der eIDAS-VO oder ein nichtqualifiziertes Authentisierungszertifikat. Die Schwelle liegt hier also niedriger als bei der Identitätsfeststellung.

Ob ein Matrix-Device-Key mit Cross-Signing (ADR-1100) oder der nachrichtenbezogene Identitätsnachweis als SD-JWT VC (ADR-1106, ADR-1107) dem Wortlaut genügt, ist offen. Funktional ist die ZaPuK-Lösung dem nichtqualifizierten Authentisierungszertifikat mindestens ebenbürtig, formal aber vom Katalog nicht erfasst. Auch hier empfiehlt sich eine Klarstellung.

3.3.4. Feststellbarkeit des Versands

Schließlich muss feststellbar sein, dass das elektronische Dokument von dem Nutzer des Postfach- und Versanddienstes versandt wurde (§ 13 Abs. 1 Nr. 4 ERVV; wortgleich § 10 Abs. 1 Nr. 5 ERVV für das eBO und § 6 Abs. 1 Nr. 4 ERVV für das beBPo). Umgesetzt wird diese Anforderung durch den vertrauenswürdigen Herkunftsnachweis. Dabei handelt es sich um eine elektronische Signatur, die an eine Nachricht angebracht wird, wenn das Versandpostfach nach Authentifizierung und Identifizierung des Postfachinhabers in einem sicheren Verzeichnisdienst geführt wird und der Postfachinhaber zum Zeitpunkt der Erstellung der Nachricht sicher an dem Postfach angemeldet ist.[376]

Für die Architektur folgt daraus eine Anforderung, die in den ADRs bislang nicht abgebildet ist. Der BGH stellt klar, dass sich die Nutzung eines sicheren Übermittlungswegs „(allein) anhand eines Prüfvermerks, Transfervermerks oder Prüfprotokolls zuverlässig erkennen“ lässt, nicht aber aus dem Dokument selbst.[377] ZaPuK muss folglich am Übergabepunkt zur Justiz ein entsprechendes, maschinell prüfbares Artefakt erzeugen oder aus der EGVP-Infrastruktur

[376] BGH, Beschluss vom 06.04.2023 – I ZB 103/22, Rn. 15; ausführlich zur technischen Ausgestaltung BAG, Beschluss vom 05.06.2020 – 10 AZN 53/20, Rn. 27.

[377] BGH, Beschluss vom 06.04.2023 – I ZB 103/22, Rn. 15; ebenso BGH, Beschluss vom 12.10.2023 – I ZB 24/23, Rn. 17.

durchreichen. Zuständig hierfür ist der Protokollkonverter (ADR-0010). Diese Anforderung ist von der Bereitstellungsbestätigung nach ADR-0018 zu trennen. Der vertrauenswürdige Herkunftsnachweis betrifft die Absendeseite und belegt, dass eine Nachricht aus einem bestimmten, identifizierten Postfach stammt. Die Bereitstellungsbestätigung betrifft die Empfangsseite und belegt den Eingang im Machtbereich des Empfängers. Beide Nachweise erfüllen unterschiedliche Funktionen und ersetzen einander nicht.

3.3.5. Ergänzende Anforderungen

Hinzu tritt die Barrierefreiheit nach § 13 Abs. 2 ERVV im Sinne der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0). Diese Anforderung deckt sich mit § 2 Abs. 7 Satz 1 OZG und § 7 Abs. 2 OZG und ist damit ohnehin einzuhalten. Wird ein Verzeichnis geführt, gelten nach § 13 Abs. 3 Satz 2 ERVV zusätzlich § 10 Abs. 2 Nr. 1 und 2 ERVV entsprechend. Das Postfach muss über eine Suchfunktion verfügen, mit der sich Inhaber besonderer elektronischer Anwalts-, Notar-, Steuerberater- und Behördenpostfächer auffinden lassen, und für diese adressierbar sein. Das Adressregister nach ADR-1111 ist daher für den Justizverkehr um die Auffindbarkeit dieser Postfacharten zu erweitern.

3.4. Einfache Signatur bleibt zwingend

Der sichere Übermittlungsweg entbindet nicht von der Signatur im Dokument. Auch bei Nutzung eines sicheren Übermittlungswegs „verlangt das Gesetz unverändert … die einfache Signatur durch die verantwortende Person“.[378] Erforderlich ist eine entzifferbare Namenswiedergabe, die den Verantwortlichen ohne Sonderwissen erkennen lässt; die bloße Berufsbezeichnung „Rechtsanwalt“ ohne Namensangabe genügt nicht.[379]

Für ZaPuK ist das mit der pseudonymen Adressierung vereinbar, weil die einfache Signatur im Dokument steht und nicht aus der Postfachadresse abgeleitet wird. Der Postfachzugang sollte

[378] BGH, Beschluss vom 25.02.2026 – VII ZB 29/24, Rn. 27.
[379] Loos, in: BeckOK IT-Recht, 22. Ed. 1.4.2025, § 130a ZPO, Rn. 20 mwN.

für ERV-Anwendungsfälle gleichwohl sicherstellen, dass eine einfache Signatur vorhanden ist, oder wenigstens darauf hinweisen. Ihr Fehlen führt zur Unwirksamkeit der Einreichung.

Zur Frage, ob signierende und versendende Person identisch sein müssen, differenziert die Rechtsprechung. Diese Differenzierung passt zur ZaPuK-Architektur.

Bei personengebundenen Postfächern ist Personenidentität Wirksamkeitsvoraussetzung. Ein aus einem persönlich zugeordneten besonderen elektronischen Anwaltspostfach versandtes, nicht qualifiziert signiertes Dokument ist nur wirksam eingereicht, wenn die das Dokument signierende und damit verantwortende Person mit der des tatsächlichen Versenders übereinstimmt.[380] Für Privatpersonen in ZaPuK ist das unproblematisch, weil clientseitig vom eigenen Endgerät gesendet wird (ADR-1100). Umgekehrt folgt daraus, dass ein technischer Nutzer für Privatpersonen nicht versenden darf.

Bei nicht personengebundenen Postfächern – besonderes elektronisches Behördenpostfach, Gesellschaftspostfach einer Berufsausübungsgesellschaft, eBO juristischer Personen – ist eine solche Identität dagegen nicht erforderlich. Es genügt der über den vertrauenswürdigen Herkunftsnachweis bestätigte Umstand, dass bei der Übersendung ein nach § 8 Abs. 1 bis 4 ERVV mit Zertifikat und Zertifikats-Passwort ausgestatteter zugangsberechtigter Beschäftigter des Postfachinhabers mit den vom Postfachinhaber zur Verfügung gestellten Zugangsdaten bei dem Verzeichnisdienst angemeldet war.[381] Die damit verbundene Unmöglichkeit der zweifelsfreien Zuordnung zu einer handelnden Person ist nach der Rechtsprechung hinzunehmen, weil die Authentizität des Dokuments hinsichtlich seiner Herkunft von der befugten Stelle gewährleistet bleibt.

Dies ist auf die ZaPuK-Funktionspostfächer nach ADR-1102 übertragbar. Sie sind nicht personengebundene Postfächer. Voraussetzung für die Übertragbarkeit ist allerdings ein Berechtigungsregime, das § 8 ERVV entspricht. Danach bestimmt der Postfachinhaber die

[380] BGH, Beschluss vom 25.02.2026 – VII ZB 29/24, Rn. 23, unter Verweis auf BGH, Beschluss vom 20.08.2025 – VII ZB 16/24, Rn. 19.

[381] BGH, Beschluss vom 16.09.2025 – VIII ZB 25/25, Rn. 29; BGH, Beschluss vom 25.02.2026 – VII ZB 29/24, Rn. 22, 24; für das eBO einer juristischen Person BAG, Urteil vom 28.01.2025 – 1 AZR 41/24, Rn. 15 f.

zugangsberechtigten natürlichen Personen und stellt ihnen Zertifikat und Passwort zur Verfügung (§ 8 Abs. 1 ERVV), kann Zugangsberechtigungen jederzeit aufheben oder einschränken (§ 8 Abs. 3 ERVV) und hat zu dokumentieren, wer wann zugangsberechtigt war (§ 8 Abs. 4 ERVV). Genau diese Funktionen leisten Berechtigungsverzeichnis (ADR-1112), Raum-Management-Service und die dort vorgesehene revisionssichere Protokollierung (ADR-1102). Ergänzend verlangt der BGH ein auswertbares Nachrichtenjournal, aus dem hervorgeht, welcher Nutzer zum Versandzeitpunkt am Postfach angemeldet war und unter welchem Benutzernamen der Versand erfolgte.[382] Ein solches Journal sollte in das Exportpaket nach ADR-1135 aufgenommen werden.

3.5. Wo eine qualifizierte Signatur gleichwohl erforderlich bleibt

Der Befund, dass ZaPuK ohne QES formwirksame Einreichungen tragen kann, gilt nicht ausnahmslos. In folgenden Konstellationen bleibt die qualifizierte Signatur erforderlich oder jedenfalls dringend zu empfehlen:

Erstens, wenn nicht die verantwortende Person selbst versendet, sondern der Versand durch ein Sekretariat oder eine andere Stelle ausgeführt wird – dies betrifft personengebundene Postfächer und ist der klassische Anwendungsfall der ersten Variante des § 130a Abs. 3 Satz 1 ZPO.[383] Zweitens, wenn die Übermittlung nicht über einen sicheren Übermittlungsweg, sondern über das elektronische Gerichts- und Verwaltungspostfach erfolgt (§ 4 Abs. 1 Nr. 2 ERVV). Drittens ist bei der Bündelung von Anhängen das Verbot der Containersignatur nach § 4 Abs. 2 ERVV zu beachten: Mehrere elektronische Dokumente dürfen nicht mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden. Viertens gilt für die Gegenrichtung – gerichtliche Dokumente – § 130b ZPO, und für die behördliche elektronische Zustellung verlangt § 5 Abs. 5 Satz 3 VwZG weiterhin die qualifizierte Signatur. Fünftens schließlich die materiell-rechtliche Schriftform: § 126a Abs. 1 BGB verlangt für die Ersetzung der gesetzlichen Schriftform die qualifizierte elektronische Signatur des Ausstellers. Der sichere Übermittlungsweg ersetzt sie nicht. Erheblich entschärft wird dieser Punkt allerdings durch den neuen § 130e

[382] BGH, Beschluss vom 16.09.2025 – VIII ZB 25/25, Rn. 32.
[383] Müller, in: Hornung/Schallbruch IT-SicherheitsR, § 27, Rn. 97.

ZPO: Ist eine empfangsbedürftige Willenserklärung, die der schriftlichen oder elektronischen Form bedarf, klar erkennbar in einem vorbereitenden Schriftsatz enthalten, der als elektronisches Dokument nach § 130a bei Gericht eingereicht und dem Empfänger zugestellt oder mitgeteilt wurde, so gilt sie als in der jeweiligen Form zugegangen – und zwar auch dann, wenn die Ersetzung der Schriftform durch die elektronische Form ausgeschlossen ist.

3.6. Formwirksamkeit und Beweiskraft fallen auseinander

Mit Blick auf das Sicherungsniveau von Zugangsnachweisen ist festzuhalten, dass Formwirksamkeit und Beweiskraft (dazu 2) unterschiedlichen Regeln folgen. Ein nur einfach signiertes, über einen sicheren Übermittlungsweg eingereichtes Dokument ist formwirksam eingereicht, erlangt aber nicht die Beweiskraft der Privaturkunde. § 371a Abs. 1 Satz 1 ZPO knüpft die entsprechende Anwendung der Vorschriften über die Beweiskraft privater Urkunden an eine qualifizierte elektronische Signatur oder eine notariell beglaubigte elektronische Unterschrift. Für öffentliche elektronische Dokumente gilt nach § 371a Abs. 3 Satz 1 ZPO-Abweichendes. Dort tritt bei qualifizierter Signatur oder qualifiziertem Siegel zusätzlich die Echtheitsvermutung nach § 437 ZPO hinzu (§ 371a Abs. 3 Satz 2 ZPO).

Für die Praxis heißt das: Wer ausschließlich auf den sicheren Übermittlungsweg setzt, reicht wirksam ein, muss im Bestreitensfall aber mit freier Beweiswürdigung und gegebenenfalls Sachverständigenbeweis rechnen. Wo es auf die Beweiskraft ankommt, bleibt die qualifizierte Signatur beziehungsweise das qualifizierte Siegel nach ADR-0017 das Mittel der Wahl.

3.7. Rechtsänderungsbedarf

Bei einer möglichen OZG-Novelle ist rechtstechnisch zu beachten, dass § 130a Abs. 4 Satz 1 Nr. 4 ZPO an das Nutzerkonto im Sinne des § 2 Abs. 5 OZG anknüpft; die Brücke vom Postfach dorthin schlägt § 2 Abs. 7 Satz 2 OZG mit der Aussage, das Postfach sei Bestandteil eines Nutzerkontos. Sollte diese Kopplung im Zuge einer OZG-Anpassung gelöst werden, wären daher die Verweisungen in der ZPO sowie parallel in § 55a Abs. 4 Satz 1 Nr. 4 VwGO, § 46c ArbGG, § 65a SGG, § 52a FGO und § 32a StPO mitzuführen.

Daneben ergeben sich folgende Empfehlungen: Der Katalog der Identifizierungsmittel in § 11 Abs. 2 Satz 2 ERVV sollte um EUDI-Wallet und European Business Wallet ergänzt werden, damit die perspektivisch vorgesehenen Authentisierungswege auch im Justizverkehr tragen. Der Katalog der Authentisierungsmittel in § 11 Abs. 3 ERVV sollte für die ZaPuK-Nachweisarchitektur geöffnet oder klarstellend erweitert werden. Und für den Protokollstandard sollte entweder durch Bekanntmachung nach § 5 ERVV oder durch Verordnungsänderung klargestellt werden, dass Matrix OSCI im Sinne des § 13 Abs. 1 Nr. 1 ERVV ersetzt.

Der rechtssicherste Weg wäre allerdings, ZaPuK zusätzlich durch Rechtsverordnung nach § 130a Abs. 4 Satz 1 Nr. 5 ZPO ausdrücklich als bundeseinheitlichen sicheren Übermittlungsweg festzulegen. Die dort genannten Voraussetzungen – Gewährleistung von Authentizität und Integrität der Daten sowie Barrierefreiheit – erfüllt die Zielarchitektur nach den vorliegenden Architekturentscheidungen. Dabei sind die Verordnungen zu koordinieren: Die ERVV ergeht durch die Bundesregierung mit Zustimmung des Bundesrates, während die Rechtsverordnung nach § 3c Abs. 2 VwVfG in der ab 1. Juli 2027 geltenden Fassung durch das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung ohne Zustimmung des Bundesrates ergeht.[384] Eine abgestimmte Festlegung der sicheren Übermittlungswege für Verwaltungsverfahren und Justiz vermeidet, dass ZaPuK in beiden Regimen unterschiedlich behandelt wird.

3.8. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Eine qualifizierte elektronische Signatur auf dem einzelnen Dokument ist für den elektronischen Rechtsverkehr nicht zwingend. ZaPuK kann als sicherer Übermittlungsweg nach § 130a Abs. 4 Satz 1 Nr. 4 ZPO in Verbindung mit § 13 ERVV die Formwirksamkeit tragen. Die Grundentscheidung, die Nachweisarchitektur nicht auf eine flächendeckende QES-Pflicht zu stützen, wird dadurch bestätigt.

[384] Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern, BGBl. 2026 I Nr. 199, Art. 1 Nr. 3, Art. 16 Abs. 4.

- Die Anbindung an den elektronischen Rechtsverkehr sollte über das Nutzerkonto nach § 2 Abs. 5 OZG erfolgen und nicht über den eBO-Weg. Nur so bleibt der Verzicht auf ein Adressregister für Privatpersonen (ADR-1111) und die bereichsspezifische pseudonyme Adressierung (ADR-1105) mit den Verordnungsanforderungen vereinbar. § 10 Abs. 1 Nr. 3 und § 13a Abs. 1 Nr. 1 ERVV stünden dem beim eBO entgegen.

- Das Identifizierungsniveau je Postfach ist nachzuhalten und für ERV-Anwendungsfälle auswertbar zu machen. Nur eID-gestützte BundID-Anmeldungen und das ELSTER-Verfahren nach § 87a Abs. 6 AO genügen § 13 Abs. 1 Nr. 2 ERVV. Anmeldungen auf niedrigem Vertrauensniveau tragen die Einreichung nicht (vgl. ADR-0014 bis ADR-0016).

- Am Übergabepunkt zur Justiz ist ein dem vertrauenswürdigen Herkunftsnachweis entsprechendes, maschinell prüfbares Artefakt zu erzeugen oder aus der EGVP-Infrastruktur durchzureichen (ADR-0010). Es ist von der Bereitstellungsbestätigung (ADR-0018) zu unterscheiden; der Herkunftsnachweis betrifft die Absendeseite, die Bereitstellungsbestätigung die Empfangsseite.

- Die einfache Signatur der verantwortenden Person im Dokument bleibt Wirksamkeitsvoraussetzung. Der Postfachzugang sollte sie für ERV-Anwendungsfälle erzwingen oder wenigstens auf ihr Fehlen hinweisen. Eine bloße Funktions- oder Berufsbezeichnung genügt nicht.

- Für Funktionspostfächer (ADR-1102) ist Personenidentität zwischen signierender und versendender Person nicht erforderlich, sofern das Berechtigungsregime dem § 8 ERVV entspricht. Berechtigungsverzeichnis (ADR-1112), revisionssichere Protokollierung und ein auswertbares Nachrichtenjournal sind daher nicht nur datenschutzrechtlich, sondern auch prozessrechtlich geboten. Das Journal sollte in das Exportpaket (ADR-1135) aufgenommen werden.

- Für Privatpersonen ist die clientseitige Terminierung der Verschlüsselung im Endgerät (ADR-1100) auch prozessrechtlich vorzugswürdig, weil hier Personenidentität

zwischen signierender und versendender Person gewahrt bleibt. Ein Versand durch technische Nutzer für Privatpersonen ist auszuschließen.

- Das Adressregister ist für den Justizverkehr um die Auffindbarkeit und Adressierbarkeit von beA, beN, beSt und beBPo zu erweitern (§ 13 Abs. 3 Satz 2 in Verbindung mit § 10 Abs. 2 Nr. 1 und 2 ERVV).

- Bei der Bündelung von Anhängen ist das Verbot der Containersignatur (§ 4 Abs. 2 ERVV) zu beachten. Das SDK (ADR-0009) sollte eine gemeinsame Signatur über mehrere Dokumente technisch ausschließen.

- Formwirksamkeit und Beweiskraft sind auseinanderzuhalten. Wo es auf die Urkundenbeweiskraft nach § 371a ZPO ankommt, bleibt die qualifizierte Signatur beziehungsweise das qualifizierte Siegel nach ADR-0017 erforderlich. Dies ist in den Zustelloptionen (ADR-1119) abbildbar.

- Es wird empfohlen, eine ausdrückliche Festlegung von ZaPuK als bundeseinheitlicher sicherer Übermittlungsweg nach § 130a Abs. 4 Satz 1 Nr. 5 ZPO anzustreben und die Verordnung mit § 3c Abs. 2 VwVfG in der ab 1. Juli 2027 geltenden Fassung abzustimmen.

- Eine etwaige Entkopplung von Postfach und Nutzerkonto im OZG muss die Verweisungen in § 130a Abs. 4 Satz 1 Nr. 4 ZPO und den Parallelvorschriften der übrigen Verfahrensordnungen synchron mitführen. Andernfalls verliert ZaPuK seine Grundlage als sicherer Übermittlungsweg.

4. Lesebestätigung als elektronisches Empfangsbekenntnis (§ 173 Abs. 3 ZPO)

Kurzzusammenfassung. Für den ganz überwiegenden Teil der ZaPuK-Anwendungsfälle wird ein Empfangsbekenntnis nicht benötigt. Bei der Zustellung an nicht berufsmäßig Beteiligte – insbesondere an Privatpersonen – knüpft § 173 Abs. 4 Satz 4 ZPO die Zustellfiktion an die automatisierte Eingangsbestätigung und damit an genau jenen Nachweis, den die Bereitstellungsbestätigung nach ADR-0018 erbringt. Eine Mitwirkung des Empfängers ist dort bewusst nicht

vorgesehen. Anders liegt es bei den in § 173 Abs. 2 ZPO genannten Empfängern, also bei Behörden, Körperschaften und Anstalten des öffentlichen Rechts sowie bei den sonstigen in professioneller Eigenschaft am Prozess beteiligten Personen und Organisationen. Für sie ist das elektronische Empfangsbekenntnis zwingend, und die Bereitstellungsbestätigung löst die Zustellung gerade nicht aus.

Die Anforderungen an ein solches Empfangsbekenntnis lassen sich in vier Punkten zusammenfassen. Es setzt eine bewusste Entgegennahmeentscheidung des Empfängers einschließlich der Eingabe eines Zustellungsdatums voraus und ist deshalb nicht automatisierbar. Es ist in dem vom Gericht mit der Zustellung übersandten strukturierten Datensatz abzugeben und an das Gericht zurückzuleiten. Eine qualifizierte elektronische Signatur ist nur erforderlich, wenn der Postfachinhaber den Versand nicht selbst vornimmt. Und der Empfänger muss eindeutig als Inhaber eines bestimmten Postfachs identifizierbar sein – ein über die Anforderungen des sicheren Übermittlungswegs hinausgehendes Vertrauensniveau verlangt das Gesetz dagegen nicht. Die in ADR-1118 vorgesehene aktive Lesebestätigung trifft damit den richtigen Ansatz, deckt die Anforderungen aber noch nicht vollständig ab; erforderlich ist ein eigenes Justizprofil, das Datumseingabe, XJustiz-Datensatz und Rücklauf über den Protokollkonverter (ADR-0010) umfasst.

4.1. Wann ein Empfangsbekenntnis verlangt wird

§ 173 ZPO unterscheidet zwei Empfängergruppen. Nach Absatz 2 haben Rechtsanwälte, Notare, Gerichtsvollzieher, Steuerberater sowie sonstige in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann, ferner Behörden, Körperschaften und Anstalten des öffentlichen Rechts einen sicheren Übermittlungsweg zu eröffnen. Diese passive Nutzungspflicht zielt darauf, alle diejenigen in den elektronischen Rechtsverkehr einzubinden, die aufgrund und im Rahmen ihrer beruflichen Tätigkeit regelmäßig mit dem Gericht kommunizieren.[385] An diese Empfänger wird die Zustellung nach Absatz 3 durch ein elektronisches Empfangsbekenntnis nachgewiesen. An alle übrigen Empfänger kann nach Absatz 4 elektronisch zugestellt werden,

[385] Wittschier, in: Musielak/Voit, ZPO, 23. Aufl. 2026, § 173, Rn. 3.

sofern sie zugestimmt haben. Dort gilt das Dokument am vierten Tag nach dem auf der automatisierten Eingangsbestätigung ausgewiesenen Tag des Eingangs im eröffneten Postfach als zugestellt, wobei der Nachweis eines fehlenden oder späteren Zugangs möglich bleibt.

Grund für diese Zweiteilung ist, dass der Zustellungsnachweis anders als bei den in Absatz 2 Genannten, die kraft Amtes ein besonderes Maß an Vertrauenswürdigkeit genießen, bei den übrigen Beteiligten nicht von einem willentlichen Akt wie der Rücksendung eines Empfangsbekenntnisses abhängen soll. Stattdessen soll die ohnehin eingehende automatische Eingangsbestätigung genutzt werden, die präzise angibt, wann das Dokument an das Postfach übermittelt und dort gespeichert wurde.[386] Dieses Modell bildet die Zielarchitektur mit der serverseitig erzeugten Bereitstellungsbestätigung nach.

Für ZaPuK ergibt sich eine entsprechende Aufteilung. Im Verhältnis zu Privatpersonen – dem Regelfall der Bürgerdomäne – genügt die Bereitstellungsbestätigung; eine Lesebestätigung ist rechtlich entbehrlich. Praktisch relevant wird das Empfangsbekenntnis dort, wo öffentliche Stellen ZaPuK als Empfangsweg nutzen, und bei denjenigen professionell Beteiligten, die weder über ein besonderes Anwalts-, Notar- noch Steuerberaterpostfach verfügen. Dieser Kreis umfasst u.a. Rentenberater, Gewerkschaften und Arbeitgebervereinigungen, Verbraucherzentralen und registrierte Inkassodienstleister. Die Rechtsprechung zählt auch öffentlich bestellte und vereidigte Sachverständige dazu und hat einer Sachverständigen aufgegeben, ein geeignetes Postfach einzurichten, wobei sie ausdrücklich auf „Mein Justizpostfach" nach dem OZG als gangbaren Weg verwiesen hat.[387] Für ZaPuK als Nachfolger dieses Postfachs ist das ein praktischer Anwendungsfall.

Von der Zustimmung nach § 173 Abs. 4 Satz 1 ZPO ist die Eröffnung des Zugangs zu unterscheiden. Die bloße Einrichtung eines besonderen elektronischen Postfachs reicht für die Annahme einer Zustimmung regelmäßig nicht aus. Erforderlich ist, dass dem Postfachinhaber die im eigenen Interesse bestehende Sorgfaltspflicht zur regelmäßigen Kontrolle des Postfachs deutlich vor Augen steht.[388] Das ist für ZaPuK bedeutsam, weil dort jede Person und jede

[386] Wittschier, in: Musielak/Voit, § 173, Rn. 6.
[387] OLG Hamm, Beschluss vom 01.07.2024 – 22 U 15/24.
[388] Wittschier, in: Musielak/Voit, § 173, Rn. 6.

Organisation ein Postfach erhält, ohne dass darin schon eine Zustimmung zur gerichtlichen Zustellung läge. Als erteilt gilt die Zustimmung erst, wenn der Inhaber den sicheren Übermittlungsweg im jeweiligen Verfahren initiativ nutzt (Satz 2).

4.2. Voluntatives Element: keine automatisierbare Quittung

Der entscheidende Unterschied zur Bereitstellungsbestätigung liegt darin, dass das Empfangsbekenntnis eine Willensentscheidung des Empfängers voraussetzt. Erforderlich ist, dass die Nachricht geöffnet, mit einer entsprechenden Eingabe ein Empfangsbekenntnis erstellt, das Datum des Erhalts eingetragen und das so erzeugte Bekenntnis versandt wird; ohne dieses aktive Zutun wird ein Empfangsbekenntnis nicht ausgelöst.[389] Zustellungsdatum ist folgerichtig nicht der Tag des Eingangs im Machtbereich, sondern der Tag, an dem der Adressat vom Zugang Kenntnis erlangt, das Dokument empfangsbereit entgegennimmt und dies durch Rücksendung bekundet.

Der Gesetzgeber hat für die in § 173 Abs. 2 ZPO Genannten bewusst daran festgehalten, den Zustellungsnachweis an ein voluntatives Element zu knüpfen, und lässt die automatisierte Eingangsbestätigung – gegebenenfalls verbunden mit einem Zeitablauf – dort gerade nicht genügen.[390] Maßgeblich ist damit das Empfangsbekenntnis und nicht das Versandprotokoll der Übermittlungsinfrastruktur.

Für ZaPuK folgt, dass die in ADR-1118 vorgesehene automatische Abrufbestätigung als Empfangsbekenntnis untauglich ist, weil ihr das Willenselement fehlt. Zudem muss die aktive Lesebestätigung so ausgestaltet sein, dass sie ein frei eingebbares Zustellungsdatum vorsieht. Dieses kann vom Abruf- oder Anzeigezeitpunkt abweichen; eine technische Vorbelegung mit dem Systemdatum oder gar ein automatischer Versand würde den Erklärungscharakter verfehlen.

[389] BGH, Beschluss vom 17.01.2024 – VII ZB 22/23, Ls. 1; ebenso BFH, Beschluss vom 03.06.2025 – VIII R 16/23, Rn. 19.

[390] BFH, Urteil vom 20.01.2026 – VII R 4/25 und VII R 5/25, jeweils Rn. 22, unter Verweis auf BVerwG, Beschluss vom 19.09.2022 – 9 B 2.22.

4.3. Form: strukturierter Datensatz und Rücklauf an das Gericht

Für die Übermittlung ist nach § 173 Abs. 3 Satz 2 ZPO der vom Gericht mit der Zustellung zur Verfügung gestellte strukturierte Datensatz zu verwenden. Nur wenn das Gericht – etwa wegen technischer Probleme – ausnahmsweise keinen solchen Datensatz bereitstellt, tritt an dessen Stelle ein elektronisches Dokument nach § 130a ZPO (§ 173 Abs. 3 Satz 3 ZPO). Der Datensatz kann durch einfaches Klicken bestätigt und als zurücklaufender Datensatz sofort dem zugestellten Dokument zugeordnet werden.[391] In der Justizinfrastruktur ist er eine XJustiz-Nachricht, deren Anforderung der zuzustellenden Nachricht beigefügt und mit ihr untrennbar verbunden ist. Der Empfänger kann sich durch Öffnen der Nachricht zuverlässig Kenntnis davon verschaffen.[392]

Für die Architektur folgt, dass das in ADR-1118 vorgesehene verschlüsselte Custom Event im Vorgangsraum als solches kein Empfangsbekenntnis ist. Es kann die Erklärung des Nutzenden entgegennehmen, ersetzt aber weder den vorgeschriebenen Datensatz noch dessen Rücklauf an das Gericht. Erforderlich ist ein Justizprofil, das die eingehende Anforderung mitsamt Datensatz bis in den Postfachzugang durchreicht, sie dort erkennbar und lesbar darstellt, die Erklärung samt Datum aufnimmt und den ausgefüllten Datensatz über den Protokollkonverter (ADR-0010) in die EGVP-Infrastruktur zurückführt. Die Darstellung ist dabei nicht nebensächlich: Sie muss die Aufforderung so hervorheben, dass eine bewusste Kenntnisnahme möglich ist und keine Verwechslungsgefahr mit der bloßen Abrufbestätigung entsteht.

4.4. Identifizierbarkeit, Signatur und Vertrauensniveau

Für eine Zustellung im prozessualen Sinne muss der Empfänger eindeutig identifizierbar sein. Dafür genügt allerdings, dass er eindeutig als Inhaber eines bestimmten Postfachs identifiziert werden kann. Das beA, beN und beBPo erfüllen diese Voraussetzung bereits;[393] ebenso auch beSt. Verlangt ist also die eindeutige Zuordenbarkeit des Postfachs, nicht die Offenlegung eines Klarnamens in der Adresse. Das ist für ZaPuK bedeutsam: Die bereichsspezifische

[391] Wittschier, in: Musielak/Voit, § 173, Rn. 5.
[392] BVerwG, Beschluss vom 19.09.2022 – 9 B 2.22, Rn. 22.
[393] Wittschier, in: Musielak/Voit, § 173, Rn. 4.

pseudonyme Adressierung (ADR-1104, ADR-1105) steht der Zustellung nicht entgegen, solange die Zuordnung des Postfachs zu seinem Inhaber über die Registrierung und – bei Organisationen – über das Adressregister (ADR-1111) belastbar nachvollziehbar bleibt. Für die Bürgerdomäne stellt sich die Frage praktisch nicht, weil dort § 173 Abs. 4 ZPO greift.

Eine qualifizierte elektronische Signatur verlangt das Gesetz für das Empfangsbekenntnis nicht. Sie ist nur erforderlich, wenn der Inhaber des besonderen elektronischen Postfachs den Versand nicht selbst vornimmt. Dann ist der Strukturdatensatz zusätzlich nach § 130a Abs. 3 ZPO qualifiziert zu signieren, denn nur der Versand über den dem Empfänger persönlich zugeordneten sicheren Übermittlungsweg erfüllt die Vorgabe.[394] Technisch abgesichert wird dies dadurch, dass die Abgabe ohne qualifizierte Signatur nur demjenigen ermöglicht wird, der als Inhaber desjenigen Postfachs angemeldet ist, an das die Aufforderung gerichtet war, und dass für den Empfänger feststellbar bleibt, ob der Postfachinhaber selbst versandt hat.[395]

Ein eigenes, gesondertes Vertrauensniveau für das Empfangsbekenntnis kennt das Recht des elektronischen Rechtsverkehrs nicht. Maßgeblich ist dasjenige Niveau, das ohnehin für den sicheren Übermittlungsweg gilt und in Abschnitt 3 dargestellt ist: Identitätsfeststellung durch ein Identifizierungsmittel nach § 11 Abs. 2 Satz 2 Nr. 1 oder 2 ERVV oder durch ein sicheres Verfahren nach § 87a Abs. 6 AO, Authentisierung beim Versand nach § 11 Abs. 3 ERVV und Feststellbarkeit, dass das Dokument vom Nutzer des Postfach- und Versanddienstes versandt wurde (§ 13 Abs. 1 ERVV). Der in ADR-1118 vorgesehene Ansatz, für das Empfangsbekenntnis eine Authentisierung mit erhöhtem Vertrauensniveau und eine qualifizierte Signatur zu verlangen, geht damit über das rechtlich Gebotene hinaus.

Für Funktionspostfächer ist bedeutsam, dass keine Identität zwischen der zustellungsempfangenden Organisation und einer bestimmten natürlichen Person verlangt wird. Bei nicht personengebundenen Postfächern genügt die Abgabe durch eine zugangsberechtigte Person. Die Praxis der behördlichen Empfangsbekenntnisse bestätigt dies.[396] Das in ADR-1102 und ADR-

[394] Wittschier, in: Musielak/Voit, § 173, Rn. 5.
[395] BSG, Urteil vom 14.07.2022 – B 3 KR 2/21 R, Rn. 14.
[396] Vgl. BFH, Urteil vom 20.01.2026 – VII R 5/25, Rn. 25, zu einem vom Hauptzollamt signierten und zurückgesandten Empfangsbekenntnis.

1112 angelegte Berechtigungs- und Protokollierungsregime trägt diese Konstellation; erforderlich ist allerdings, dass sich im Nachhinein feststellen lässt, wer zum Zeitpunkt der Abgabe zugangsberechtigt und angemeldet war.

4.5. Beweiskraft und Folgen des Ausbleibens

Das elektronisch abgegebene Empfangsbekenntnis erbringt – wie das papiergebundene – gegenüber dem Gericht den vollen Beweis nicht nur für die Entgegennahme des Dokuments als zugestellt, sondern auch für den angegebenen Zeitpunkt und damit für die Zustellung.[397] Der Gegenbeweis ist zulässig, setzt aber voraus, dass die Beweiswirkung vollständig entkräftet und jede Möglichkeit ausgeschlossen ist, dass die Angaben richtig sein könnten. Damit erreicht das Empfangsbekenntnis eine Beweisstufe, die die Bereitstellungsbestätigung aus eigener Kraft nicht erreicht.

Bleibt die Rücksendung aus, gelten dieselben Rechtsfolgen wie beim nicht zurückgesandten Empfangsbekenntnis in Papierform. Der Zustellungsmangel wird nach § 189 ZPO geheilt, wenn neben dem tatsächlichen Zugang die Empfangsbereitschaft anderweitig festgestellt werden kann. Der Tag der Entgegennahme mit Empfangswillen kann dann mit den zur Verfügung stehenden Beweismitteln nachgewiesen werden.[398] Ob dafür bereits die automatische Eingangsbestätigung genügt, ist höchstrichterlich noch nicht abschließend geklärt; das Bundesverwaltungsgericht hat die Revision zu dieser Frage zugelassen.[399] Hier liegt der Wert der übrigen ZaPuK-Nachweise: Bereitstellungsbestätigung und automatische Abrufbestätigung belegen den Eingang im Postfach und die erfolgreiche Entschlüsselung und stützen damit die Feststellung des tatsächlichen Zugangs (wenn das Postfach im Machtbereich des Empfängers verortet werden kann, siehe auch Vorbemerkung zu 2). Die Empfangsbereitschaft können sie nicht beweisen; sie sind Hilfsmittel zur Heilung, nicht Ersatz des Empfangsbekenntnisses.

Dass die Abgabe technisch nicht erzwingbar ist, wie ADR-1118 zutreffend feststellt, ist rechtlich unbedenklich. Auch das Gesetz erzwingt sie nicht, sondern begegnet ihrem Ausbleiben über

[397] BGH, Beschluss vom 17.01.2024 – VII ZB 22/23, Ls. 2.
[398] BFH, Beschluss vom 03.06.2025 – VIII R 16/23, Rn. 21.
[399] BVerwG, Beschluss vom 26.07.2024 – 5 B 23.23, Rn. 2.

§ 189 ZPO und das Wiedereinsetzungsrecht. Für die in § 173 Abs. 2 ZPO Genannten besteht allerdings eine Mitwirkungsobliegenheit, deren Verletzung Verschuldensfolgen auslösen kann. Für Behörden gelten dabei dieselben Sorgfaltsmaßstäbe wie für die rechts- und steuerberatenden Berufe.[400] Postfachzugänge, die von diesen Empfängern genutzt werden, müssen die Funktion daher bereitstellen. Das ist über die Anschlussbedingungen abzusichern.

4.6. Übertragbarkeit auf die behördliche Zustellung

Für die förmliche Zustellung durch Behörden gilt eine strukturell parallele Regelung. Nach § 5 Abs. 4 und 5 VwZG kann elektronisch gegen Empfangsbekenntnis zugestellt werden; zum Nachweis genügt nach § 5 Abs. 7 Satz 1 VwZG das mit Datum und Unterschrift versehene Empfangsbekenntnis, das elektronisch zurückzusenden ist. Ein vorgeschriebener strukturierter Datensatz existiert dort nicht, sodass die Anforderungen geringer sind als im gerichtlichen Verfahren. Ein Justizprofil, das die Anforderungen des § 173 Abs. 3 ZPO erfüllt, deckt die verwaltungsrechtliche Variante daher mit ab. Zu beachten bleibt, dass § 5 Abs. 5 Satz 3 VwZG für das zuzustellende Dokument selbst – nicht für das Empfangsbekenntnis – weiterhin die qualifizierte Signatur verlangt.

4.7. Folgerungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

- Für Privatpersonen ist eine Lesebestätigung im elektronischen Rechtsverkehr rechtlich nicht erforderlich. Die Zustellfiktion des § 173 Abs. 4 Satz 4 ZPO knüpft an die automatisierte Eingangsbestätigung an, die durch die Bereitstellungsbestätigung nach ADR-0018 erbracht wird. Dies stützt die Grundentscheidung, die Beweiskette auf den serverseitigen Nachweis zu stützen.
- Für Empfänger nach § 173 Abs. 2 ZPO – öffentliche Stellen und professionell Beteiligte – genügt die Bereitstellungsbestätigung nicht. Dort löst erst das Empfangsbekenntnis

[400] BFH, Urteil vom 20.01.2026 – VII R 5/25, Rn. 24.

die Zustellung und damit den Fristlauf aus. Dies ist in ADR-1118 und in der Beweiskettendarstellung des Architekturkonzepts (Abschnitt 5.4.12) klarzustellen.

- Die aktive Lesebestätigung ist um ein frei eingebbares Zustellungsdatum zu ergänzen. Eine Vorbelegung mit dem Abruf- oder Systemdatum sowie jede Form des automatischen Versands sind zu vermeiden, weil sie das voluntative Element beeinträchtigen können. Das Feld kann und sollte jedoch als Pflichtfeld ausgestattet sein, da das Datum ein vorgeschriebenes Element des Empfangsbekenntnisses ist; ebenso erscheint es unschädlich und sinnvoll, wenn das Feld nur Datumseingaben akzeptiert.

- Das verschlüsselte Custom Event ersetzt den vorgeschriebenen strukturierten Datensatz nicht. Erforderlich ist ein Justizprofil, das die XJustiz-Anforderung durchreicht, im Postfachzugang erkennbar darstellt und den ausgefüllten Datensatz über den Protokollkonverter (ADR-0010) an das Gericht zurückführt. Der Rücklauf ist in das Exportpaket nach ADR-1135 aufzunehmen.

- Die pseudonyme Adressierung (ADR-1104, ADR-1105) steht der Zustellung nicht entgegen. Verlangt ist die eindeutige Identifizierbarkeit als Postfachinhaber, nicht ein Klarname in der Adresse. Die Zuordnung des Postfachs zu seinem Inhaber muss über Registrierung und Adressregister (ADR-1111) belastbar nachvollziehbar bleiben.

- Eine qualifizierte elektronische Signatur ist keine Wirksamkeitsvoraussetzung, solange der Postfachinhaber selbst aus seinem Postfach versendet. Sicherzustellen ist stattdessen, dass die Abgabe nur dem angemeldeten Postfachinhaber möglich ist und dass die Herkunft aus dessen Postfach für den Empfänger feststellbar bleibt. Dies deckt sich mit § 13 Abs. 1 Nr. 4 ERVV. Für den Versand durch Dritte ist die Möglichkeit einer qualifizierten Signatur des Datensatzes vorzusehen.

- Ein gegenüber dem sicheren Übermittlungsweg erhöhtes Vertrauensniveau verlangt das Gesetz nicht. Die entsprechende Vorgabe in ADR-1118 sollte als optionale Verschärfung und nicht als Wirksamkeitsvoraussetzung formuliert werden.

- Bereitstellungs- und Abrufbestätigung behalten auch dort ihren Wert, wo ein Empfangsbekenntnis ausbleibt: Sie stützen die Heilung nach § 189 ZPO, ersetzen aber den Nachweis der Empfangsbereitschaft nicht. Die Reichweite dieser unterstützenden Wirkung ist höchstrichterlich im Detail noch offen.[401]

- Die bloße Bereitstellung eines Postfachs begründet keine Zustimmung nach § 173 Abs. 4 Satz 1 ZPO. Postfachzugänge sollten die aus der Nutzung folgende Kontrollobliegenheit sichtbar machen. Die Zustimmungsfiktion greift erst mit initiativer Nutzung im jeweiligen Verfahren.

5. Zulassung zum elektronischen Rechtsverkehr und Vereinbarkeit mit dem risikobasierten Anschlussverfahren

Kurzzusammenfassung. Zu trennen sind Teilnehmer- und Backend-Ebene. Auf der Teilnehmerebene regelt § 7 ERVV die Identitätsprüfung des Postfachinhabers – allerdings nur für das besondere elektronische Behördenpostfach. Für den für ZaPuK maßgeblichen Weg über § 130a Abs. 4 Satz 1 Nr. 4 ZPO in Verbindung mit § 13 ERVV gibt es eine solche Prüfstelle nicht. Die Identitätsfeststellung ist dort nicht organisations-, sondern mittelbezogen geregelt und der Katalog des § 11 Abs. 2 Satz 2 Nr. 1 und 2 ERVV ist abschließend. Eine verwaltungsinterne Zulassung analog § 7 ERVV ist für diesen Weg daher weder erforderlich noch genügend.

Auf der Backend-Ebene kennt die ERVV überhaupt kein Zulassungs-, Akkreditierungs- oder Zertifizierungsverfahren. Die Anforderungen des § 13 Abs. 1 ERVV sind objektive Wirksamkeitsvoraussetzungen, die das Gericht im Streitfall inzident prüft. Eine Zulassung hätte weder konstitutive noch heilende Wirkung. Daraus folgt für ADR-1145: Der risikobasierte Ansatz bleibt im Grundsatz tragfähig, für die ERV-relevanten Anforderungen versagen aber die Zusicherungsarten „strukturell", „erkennbar" und „vertraglich". Die ERV-Fähigkeit ist als eigene, vorab geprüfte Anschlussstufe auszugestalten.

[401] BVerwG, Beschluss vom 26.07.2024 – 5 B 23.23.

5.1. Kein Zulassungsverfahren für den Übermittlungsweg

Die ERVV formuliert die Anforderungen an den Postfach- und Versanddienst eines Nutzerkontos rein konditional: Der Dienst „kann genutzt werden, wenn" die vier Voraussetzungen des § 13 Abs. 1 ERVV vorliegen. Weder ist eine Stelle benannt, die diese Voraussetzungen feststellt, noch ist eine Aufsicht, ein Konformitätsbewertungsverfahren oder ein Register der zugelassenen Dienste vorgesehen. Das unterscheidet den ERV deutlich vom De-Mail-Regime mit seiner Akkreditierung und von den qualifizierten Vertrauensdiensten nach der eIDAS-VO, deren Status durch die Aufsichtsstelle verliehen wird.

Ob ZaPuK ein sicherer Übermittlungsweg ist, ergibt sich somit nicht aus einer vorgeschalteten Zulassungsentscheidung, sondern wird im konkreten Verfahren durch das erkennende Gericht anhand des Prüf- oder Transfervermerks entschieden. Eine verbundinterne Zulassung könnte diese Prüfung weder ersetzen noch vorwegnehmen. Umgekehrt heilt sie einen Mangel nicht.

5.2. § 7 ERVV trägt für den ZaPuK-Weg nicht

§ 7 ERVV beschreibt ein rein verwaltungsinternes Verfahren. Eine von den obersten Bundesbehörden oder den Landesregierungen bestimmte öffentlich-rechtliche Stelle prüft, ob der Postfachinhaber eine inländische Behörde oder juristische Person des öffentlichen Rechts ist und ob Name und Sitz zutreffend bezeichnet sind, und bestätigt dies im sicheren elektronischen Verzeichnis. Für Behörden, die über ein beBPo nach § 130a Abs. 4 Satz 1 Nr. 2 ZPO einreichen, bleibt dies der maßgebliche Weg.

Für den über § 13 ERVV vermittelten Weg gilt das nicht. Dort ist die Identität durch ein Identifizierungsmittel nach § 11 Abs. 2 Satz 2 Nr. 1 oder 2 ERVV oder durch ein nach § 87a Abs. 6 AO in der Steuerverwaltung eingesetztes sicheres Verfahren festzustellen. Zulässig sind damit ausschließlich der elektronische Identitätsnachweis, ein qualifiziertes elektronisches Siegel nach Art. 38 eIDAS-VO sowie das ELSTER-Verfahren. Eine behördliche Identitätsbestätigung nach § 7 ERVV ist in diesem Katalog nicht enthalten. Öffentliche Stellen, die über ZaPuK am ERV teilnehmen sollen, benötigen daher praktisch ein qualifiziertes elektronisches Siegel. Die im Architekturkonzept vorgesehene Nutzung von Verwaltungs-PKI-Zertifikaten genügt nur, soweit sie

diese Qualität erreicht. Naheliegend und regelungstechnisch schlank wäre, § 13 Abs. 1 Nr. 2 ERVV um die Bestätigung nach § 7 ERVV zu ergänzen – dann könnte die vorhandene Prüfstellenstruktur der Länder für die Organisations- und Behörden-Backends nachgenutzt werden.

5.3. Unzulänglichkeit der risikobasierten Zusicherung für den ERV

ADR-1145 stuft die Anschlussbedingungen danach ab, wen ein Verstoß trifft und ob er beobachtbar ist. Für die ERV-Anforderungen führt diese Systematik zu einem anderen Ergebnis als für die übrigen Bedingungen. Ein Verstoß schädigt gerade nicht überwiegend die eigene Organisation, sondern den Absender, der auf die Formwirksamkeit seiner Einreichung vertraut. Das Sächsische Oberverwaltungsgericht hat für ein nicht konform konfiguriertes Behördenpostfach entschieden, dass die fehlende Übermittlung des vertrauenswürdigen Herkunftsnachweises die Einreichung unwirksam macht, dass es der absendenden Stelle obliegt, durch geeignete organisatorische und technische Maßnahmen sicherzustellen, dass nur formwirksame Dokumente ihren Machtbereich verlassen, und dass die bloße Unkenntnis eines solchen Systemfehlers – auch bei Betreuung durch beauftragte externe IT-Dienstleister – nicht entlastet.[402] Der BGH betont ergänzend, dass sich die Nutzung eines sicheren Übermittlungswegs allein anhand des Prüf- oder Transfervermerks feststellen lässt.

Damit greift die risikobasierte Zusicherung zu kurz. Der Mangel wird zwar sichtbar, aber typischerweise erst mit dem gerichtlichen Hinweis und damit regelmäßig nach Fristablauf. Die Hinweispflicht nach § 130a Abs. 6 ZPO und ihren Parallelvorschriften hilft nicht, weil sie nach gefestigter Rechtsprechung eng auszulegen ist und nur die Bearbeitungseignung, nicht die wirksame Übermittlung betrifft. Die Zusicherungsart vertraglich versagt, weil ein Haftungsanspruch gegen den Backend-Betreiber eine versäumte prozessuale Frist nicht heilt.

5.4. Empfehlungen für die Architektur von ZaPuK

Für die Architektur von ZaPuK ergibt sich aus dem Vorstehenden:

[402] Beschluss vom 20.12.2019 – 5 A 1048/19.A.

- Die ERV-Fähigkeit sollte in ADR-1145 als eigene Anschlussstufe geführt werden, für die die Konformitätsprüfung im Einzelfall nicht Ausnahme, sondern Regel ist. Vor der Freischaltung sind Protokollstandard, Identifizierungsmittel, Authentisierung beim Versand und die Erzeugung eines dem vertrauenswürdigen Herkunftsnachweis entsprechenden Artefakts (§ 13 Abs. 1 Nr. 1 bis 4 ERVV) verifiziert nachzuweisen. Eine Eigenerklärung genügt nicht.

- Die Föderationsliste sollte die ERV-Fähigkeit je Backend ausweisen, und der Postfachzugang sollte vor dem Versand an ein Gericht erkennbar machen, ob der gewählte Weg diese Eigenschaft trägt. Nur so kann der Absender die ihm obliegende Ausgangskontrolle überhaupt erfüllen.

- Suspendierung und Ausschluss dürfen für den ERV nicht ohne Vorlauf wirken. Da der Verlust der ERV-Fähigkeit unmittelbar Fristen gefährdet, sind Vorankündigung, Übergangsfrist und eine unmittelbare Warnung der betroffenen Absender vorzusehen; die Historie der ERV-Fähigkeit ist vorzuhalten, damit sich die Konformität zum Versandzeitpunkt später belegen lässt.

- Für öffentliche Stellen ist sicherzustellen, dass die Identitätsfeststellung über eines der abschließend zugelassenen Mittel erfolgt, praktisch über ein qualifiziertes elektronisches Siegel. Ergänzend wird angeregt, § 13 Abs. 1 Nr. 2 ERVV um die Bestätigung nach § 7 ERVV zu erweitern.

- Rechtssicherheit lässt sich abschließend nur durch Rechtsetzung herstellen. Die bereits in Abschnitt 3 empfohlene Festlegung von ZaPuK als bundeseinheitlicher sicherer Übermittlungsweg durch Rechtsverordnung nach § 30a Abs. 4 Satz 1 Nr. 5 ZPO sollte daher zugleich genutzt werden, um ein Zulassungsverfahren und dessen Rechtsfolgen zu normieren. Damit würde die verbundinterne Zulassung von einer bloß vertraglichen zu einer rechtlich tragenden Entscheidung.

VII. Weitere Einzelfragen

1. Rechtsfolgen unzustellbarer oder fehlerhaft verschlüsselter Nachrichten

Vor dem Hintergrund der datenschutzrechtlich gebotenen (siehe III.3.6.2) und auch TK-rechtlich motivierten Verschlüsselung stellt sich die Frage nach den rechtlichen Konsequenzen, die eintreten, wenn eine über die zentrale Postfachinfrastruktur übermittelte Nachricht beim Empfänger nicht entschlüsselt und damit nicht zur Kenntnis genommen werden kann. Praktisch geht es um Konstellationen wie den Verlust oder die Sperrung des privaten Schlüssels, fehlerhafte Client-Konfigurationen, defekte Signatur- oder Verschlüsselungstoken sowie systemseitige Fehler in der Ver- oder Entschlüsselungskette.

Im Ausgangspunkt ist davon auszugehen, dass sich Verschlüsselungsfehler auf die Wirksamkeit der Bekanntgabe beziehungsweise Zustellung auswirken und vom Empfänger prozessual mit Erfolg geltend gemacht werden können. Der Grund liegt im Zugangsbegriff selbst: Ein elektronisches Dokument geht erst zu, wenn es in den Machtbereich des Empfängers gelangt und von diesem unter gewöhnlichen Umständen zur Kenntnis genommen werden kann. Für das Steuerverfahren ist dies in § 87a Abs. 1 Satz 3 AO ausdrücklich geregelt: Ein elektronisches Dokument ist zugegangen, sobald die für den Empfang bestimmte Einrichtung des Empfängers es „in für den Empfänger bearbeitbarer Weise“ aufgezeichnet hat. Ein dauerhaft verschlüsseltes, mangels Schlüssel nicht lesbares Chiffrat ist gerade keine bearbeitbare Aufzeichnung; der Zugang ist dann nicht bewirkt. Dieser Gedanke lässt sich auf die parallelen Bekanntgaberegime des allgemeinen und des sozialen Verwaltungsverfahrens übertragen.

1.1. Abhängigkeit vom Bekanntgabemodell

Die konkreten Rechtsfolgen hängen davon ab, welches Grundmodell der Bekanntgabe die Infrastruktur im Einzelfall bedient. Zu unterscheiden sind die elektronische Übermittlung mit Bekanntgabe- oder Zustellungsfiktion, die Bereitstellung zum Abruf über ein Postfach sowie die Übermittlung gegen Abholbestätigung. Für jedes Modell stellt sich dieselbe Doppelfrage: ob sich der Empfänger auf die fehlende tatsächliche Entschlüsselbarkeit berufen kann und wer die Darlegungs- und Beweislast trägt.

1.1.1. Elektronische Übermittlung mit Fiktion

Im allgemeinen Verwaltungsverfahren gilt ein elektronisch übermittelter Verwaltungsakt nach § 41 Abs. 2 Satz 2 VwVfG am vierten Tag nach der Absendung als bekannt gegeben. Diese Fiktion ist widerlegbar: Nach § 41 Abs. 2 Satz 3 VwVfG gilt sie nicht, wenn der Verwaltungsakt nicht oder zu einem späteren Zeitpunkt zugegangen ist, und im Zweifel hat die Behörde den Zugang und den Zeitpunkt des Zugangs nachzuweisen. Im Prozess ist die Darlegungslast des Bekanntgabeadressaten gering. Ein Zweifelsfall liegt grundsätzlich schon dann vor, wenn der behauptet, den VA nicht erhalten zu haben (siehe II.2.2.1);[403] nur ausnahmsweise ist ein substantiiertes Bestreiten des Zugangs erforderlich, etwa wenn sich aus dem Verhalten des Adressaten ergibt, dass er den Inhalt des Verwaltungsakts kennt.[404] Diese geringe Darlegungslast gilt auch bei elektronisch übermittelten Verwaltungsakten, zumal der Empfänger im Allgemeinen wenig Möglichkeiten hat, den Nichtzugang zu beweisen.

Der Behauptung des Nichterhalts dürfte es bei einem elektronisch übermittelten Verwaltungsakt gleichstehen, wenn der Adressat vorträgt, dass die Nachricht mangels Entschlüsselbarkeit nicht lesbar zugegangen ist. Jedenfalls dürfte ein nachvollziehbar geschilderter Schlüsselverlust oder ein dokumentierter Entschlüsselungsfehler ausreichen, um die Zweifelsregelung auszulösen. Begründet der Vortrag des Empfängers Zweifel, trägt anschließend die Behörde die Beweislast für den tatsächlichen Zugang.

Für das Sozialverwaltungsverfahren enthält § 37 Abs. 2 SGB X und für das Besteuerungsverfahren § 122 Abs. 2a AO eine wortgleiche Regelung einschließlich der Zweifelsregelung zulasten der Behörde. Im Steuerrecht wird dieser Befund durch § 87a Abs. 2 Satz 2 AO flankiert: Macht ein Empfänger geltend, er könne das von der Finanzbehörde übermittelte Dokument nicht bearbeiten, so hat sie es ihm erneut in einem geeigneten Format oder als Schriftstück zu übermitteln. Die Nichtentschlüsselbarkeit ist damit nicht nur ein Zugangshindernis, sondern löst zugleich eine Pflicht zur erneuten Übermittlung aus.

[403] Tegethoff, in: Kopp/Ramsauer, 27. Aufl. 2026, § 41, Rn. 42b.
[404] Tegethoff, in: Kopp/Ramsauer, 27. Aufl. 2026, § 41, Rn. 42c.

Bei der förmlichen Zustellung führt § 5 Abs. 5 VwZG die elektronische Zustellung, für die das Dokument mit einer qualifizierten elektronischen Signatur zu versehen und gegen unbefugte Kenntnisnahme Dritter zu schützen ist. Der Nachweis erfolgt vorrangig über das Empfangsbekenntnis (§ 5 Abs. 7 Satz 1 VwZG). Geht dieses nicht ein, gilt das Dokument nach § 5 Abs. 7 Satz 2 VwZG am vierten Tag nach der Absendung als zugestellt. Hier ist die Verteilung strenger als im Bekanntgaberecht: Die Fiktion entfällt nur, wenn der Empfänger nachweist, dass das Dokument nicht oder erst später zugegangen ist (§ 5 Abs. 7 Satz 3 VwZG). Eine Zweifelsregelung zugunsten des Empfängers besteht nicht; er trägt die volle Beweislast für den Nichtzugang. Ein Verschlüsselungsfehler, der die Lesbarkeit verhindert, ist auch hier ein tauglicher Anknüpfungspunkt, muss vom Empfänger aber positiv belegt werden.

1.1.2. Bereitstellung zum Abruf über ein Postfach

Wird der Verwaltungsakt nicht übersandt, sondern zum Abruf bereitgestellt, verschiebt sich der Fehleransatzpunkt vom Übertragungsweg auf die Speicher- und Abrufumgebung. § 41 Abs. 2a VwVfG verlangt, dass die Behörde gewährleistet, dass der elektronische Verwaltungsakt von der berechtigten Person gespeichert werden kann; der Verwaltungsakt gilt am Tag nach dem Abruf als bekanntgegeben und die Bereitstellung endet bei Ausbleiben eines Abrufs nach zehn Tagen (in diesem Fall ist die Bekanntgabe nicht bewirkt; erneute Bereitstellung oder Bekanntgabe auf anderem Weg bleiben möglich). § 37 Abs. 2a SGB X knüpft demgegenüber an die Benachrichtigung an: Der bereitgestellte Verwaltungsakt gilt am vierten Tag nach Absendung der Benachrichtigung als bekannt gegeben, wobei die Behörde im Zweifel den Zugang der Benachrichtigung nachweisen muss; gelingt ihr das nicht, gilt der Verwaltungsakt erst am Tag des tatsächlichen Abrufs als bekannt gegeben.

Im Steuerverfahren regelt § 122a AO in Verbindung mit § 87a Abs. 8 AO die Bekanntgabe durch Bereitstellung zum Datenabruf. Dabei ist ein sicheres Verfahren zu verwenden, das die verantwortliche Stelle authentifiziert sowie Vertraulichkeit und Integrität des Datensatzes gewährleistet; die abrufberechtigte Person hat sich zu authentisieren. Der bereitgestellte Verwaltungsakt gilt nach § 122a Abs. 4 AO am vierten Tag nach der Bereitstellung als bekannt gegeben, und im Zweifel hat die Behörde den Zeitpunkt der Bereitstellung nachzuweisen. Für die zentrale

Postfachinfrastruktur besonders einschlägig ist § 9 OZG, der die Bekanntgabe über das Postfach des Nutzerkontos regelt: Auch dort muss die Behörde gewährleisten, dass der Verwaltungsakt gespeichert werden kann, es gilt eine Vier-Tage-Fiktion ab Bereitstellung, und im Zweifel hat die Behörde die Bereitstellung und deren Zeitpunkt nachzuweisen.

Für die hier interessierende Fehlerkonstellation folgt daraus ein doppelter Ansatzpunkt zugunsten des Empfängers. Zum einen kann er geltend machen, dass die gesetzlich geforderte Speicher- und Abrufbarkeit gerade nicht gewährleistet war, weil das bereitgestellte Dokument mangels entschlüsselbarem Zugriff nicht in lesbarer Form gespeichert werden konnte; dann ist bereits die Wirksamkeitsvoraussetzung der Bereitstellung nicht erfüllt. Zum anderen kann er die Fiktion an der Benachrichtigung oder – im OZG- und AO-Modell – an der Bereitstellung selbst angreifen, für die die Behörde die Beweislast trägt.

1.2. Zusammenfassende Bewertung der Fehlerfolgen

Über alle Modelle hinweg gilt: Ein Verschlüsselungsfehler, der die Lesbarkeit beim Empfänger dauerhaft verhindert, steht dem wirksamen Zugang entgegen, weil das Dokument nicht in bearbeitbarer und wahrnehmbarer Form in den Machtbereich des Empfängers gelangt. Die praktische Durchschlagskraft dieses Einwands hängt allein von der Beweislastverteilung ab. In den Bekanntgaberegimen des VwVfG, SGB X und der AO wirkt eine Zweifelsregelung zugunsten des Empfängers: Substantiierter Vortrag verlagert die Beweislast für den Zugang auf die Behörde. In den förmlichen Zustellungsregimen des VwZG (§ 5 Abs. 7, § 5a Abs. 4) trägt demgegenüber der Empfänger die volle Nachweislast für den Nichtzugang. Für die Behörde bedeutet dies umgekehrt ein doppeltes Risiko: Zum einen kann die Fiktion widerlegt werden, sodass Fristen nicht zu laufen beginnen und Verwaltungsakte nicht bestandskräftig werden. Zum anderen kann – wie § 87a Abs. 2 Satz 2 AO zeigt – eine Pflicht zur erneuten, geeigneten Übermittlung entstehen.

1.3. eIDAS als Instrument der Fehlervermeidung und Vermutungswirkung

Der Einsatz qualifizierter Vertrauensdienste nach der eIDAS-VO ist geeignet, die beschriebenen Beweisrisiken zu reduzieren, weil er gerade die Integrität und die Nachweisbarkeit von

Absendung und Empfang absichert. Ein Dienst für die Zustellung elektronischer Einschreiben ist nach Art. 3 Nr. 36 eIDAS-VO ein Dienst, der die Übermittlung von Daten zwischen Dritten ermöglicht, einen Nachweis der Handhabung einschließlich Absendung und Empfang erbringt und die Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt; die qualifizierte Ausprägung setzt zusätzlich die Anforderungen des Art. 44 eIDAS-VO voraus (unter anderem hohe Identifizierungssicherheit von Absender und Empfänger sowie Sicherung durch fortgeschrittene Signatur oder Siegel, die unbemerkte Veränderungen ausschließt).

Wird ein solcher qualifizierter Dienst genutzt, greift die Vermutungswirkung des Art. 43 Abs. 2 eIDAS-VO: Vermutet werden die Unversehrtheit der Daten, die Absendung durch den identifizierten Absender, der Empfang durch den identifizierten Empfänger sowie die Korrektheit von Datum und Uhrzeit der Absendung und des Empfangs. Umgekehrt darf nach Art. 43 Abs. 1 eIDAS-VO auch einem nichtqualifizierten Dienst die Rechtswirkung und die Zulässigkeit als Beweismittel nicht allein deshalb abgesprochen werden, weil die Anforderungen an qualifizierte Dienste nicht erfüllt sind. Für die Architektur der zentralen Postfachinfrastruktur folgt daraus, dass eine qualifizierte, eIDAS-konforme Zustellkomponente die Beweisführung der Behörde erheblich erleichtert; sie ändert allerdings nichts daran, dass die Vermutung des Art. 43 Abs. 2 eIDAS-VO auf die technische Handhabung durch den Dienst bezogen ist und die Frage der tatsächlichen Entschlüsselbarkeit beim Empfänger nicht vollständig verdrängt.

1.4. Folgerungen für die Architektur von ZaPuK

Die rechtliche Analyse legt nahe, die Infrastruktur so auszugestalten, dass Verschlüsselungsfehler entweder verhindert oder revisionssicher dokumentiert werden.

- Empfehlenswert ist erstens die Nutzung qualifizierter Vertrauensdienste im Sinne der Art. 43, 44 eIDAS-VO, um die Vermutungswirkung für Integrität, Absendung und Empfang zu erlangen.
- Zweitens sollte die Plattform die tatsächliche Speicher- und Abrufbarkeit des lesbaren Dokuments protokollieren, weil die Abruf- und Bereitstellungsmodelle (§ 41 Abs. 2a VwVfG, § 37 Abs. 2a SGB X, § 122a AO, § 9 OZG) an diese Voraussetzung anknüpfen.

- Drittens empfiehlt sich ein automatisierter Fehlerrückkanal, der eine fehlgeschlagene Entschlüsselung erkennt und – parallel zur gesetzlichen Wertung des § 87a Abs. 2 Satz 2 AO – eine erneute Bereitstellung in geeignetem Format anstößt, bevor eine Fiktion greift.

Auf diese Weise lässt sich das Risiko unwirksamer Bekanntgaben und die damit verbundene Fristen- und Bestandskraftunsicherheit für die anschließenden Behörden spürbar reduzieren.

2. Fortlaufende Bereitstellungspflicht nach Abruf

Kurzzusammenfassung. Nach dem geltenden Recht besteht keine allgemeine Pflicht, elektronische Nachrichten nach ihrem Abruf bzw. nach bewirkter Bekanntgabe langfristig im Nutzer-Postfach vorzuhalten. Rechtlich entscheidend ist der einmalige Zugangs- bzw. Zustellungsvorgang; ist dieser bewirkt, hat das Postfach seine gesetzliche Funktion erfüllt. Die dauerhafte Sicherung des Vorgangs liegt in der behördlichen Sphäre (Akten- und Archivrecht), nicht im Empfängerpostfach. Umgekehrt setzen das Datenschutzrecht (Grundsätze der Datenminimierung und Speicherbegrenzung, Art. 5 DSGVO) und – für Verkehrsdaten – das TK-Datenschutzrecht (§ 9 TDDDG) einer zeitlich unbegrenzten Vorhaltung Grenzen. Die Vorhaltedauer im Empfängerpostfach ist damit im Kern eine Frage der Dienst- und Vertragsgestaltung, die sich innerhalb dieser datenschutz- und TK-rechtlichen Leitplanken bewegen muss. Punktuelle gesetzliche Mindestvorhaltungspflichten (De-Mail-G) zeigen jedoch, dass eine sachgerechte Regelung auch die berechtigten Interessen und Erwartungen der Nutzer abbilden sollte.

2.1. Ausgangspunkt: Funktion des Postfachs

Das Postfach im Sinne des OZG ist eine IT-Komponente, über die Nutzer „vorgangsbezogen" mit den angeschlossenen öffentlichen Stellen kommunizieren sowie elektronische Dokumente senden und empfangen können (§ 2 Abs. 7 OZG); es ist Bestandteil des Nutzerkontos (§ 2 Abs. 5, Abs. 7 Satz 2 OZG). Gesetzlich definiert ist damit eine Kommunikations- und Zugangsfunktion, nicht eine dauerhafte Archiv- oder Ablagefunktion. Ein Anspruch der Nutzer auf zeitlich unbegrenzte Bereithaltung abgerufener Nachrichten lässt sich aus dieser Zweckbestimmung nicht ableiten.

2.2. Verwaltungsverfahrensrecht: Der jeweilige Vorgang/Zeitpunkt ist maßgeblich

Für die elektronische Bekanntgabe von Verwaltungsakten über ein Postfach knüpft das Gesetz an einen punktuellen Vorgang an, nicht an eine Dauerbereitstellung. Nach § 9 Abs. 1 OZG kann ein elektronischer Verwaltungsakt mit Einwilligung des Nutzers dadurch bekannt gegeben werden, dass er über dessen Postfach abgerufen wird; der Verwaltungsakt „gilt am vierten Tag nach der Bereitstellung zum Abruf als bekannt gegeben" (§ 9 Abs. 1 Satz 4 OZG). Die Behörde hat lediglich zu gewährleisten, dass der Abruf authentifiziert erfolgt und der Verwaltungsakt vom Nutzer gespeichert werden kann (§ 9 Abs. 1 Satz 3 OZG). Das Gesetz verlangt also die *Speicherbarkeit* auf Nutzerseite, nicht eine fortdauernde Vorhaltung im Postfach.

Parallel dazu regeln § 41 Abs. 2a VwVfG und § 37 Abs. 2a SGB X die Bekanntgabe durch Abruf über öffentlich zugängliche Netze. Auch dort ist der maßgebliche Rechtsakt der Zugang/Abruf: § 41 Abs. 2a Satz 3 VwVfG lässt den Verwaltungsakt „am Tag nach dem Abruf" als bekannt gegeben gelten und ordnet – als gegenläufige Wertung – sogar die Beendigung der Bereitstellung an, wenn nicht innerhalb von zehn Tagen nach Benachrichtigung abgerufen wird (§ 41 Abs. 2a Satz 4 VwVfG). Der Gesetzgeber geht mithin von einer *befristeten* Bereitstellung aus, nicht von einer dauerhaften. Nach ebenfalls einheitlicher Wertung verlangen die Vorschriften jeweils nur die Gewährleistung, dass der Verwaltungsakt „von ihr gespeichert werden kann" (§ 41 Abs. 2a Satz 2 VwVfG; § 37 Abs. 2a Satz 3 SGB X).

2.3. Dauerhafte Sicherung liegt in der behördlichen Sphäre (Akten- und Archivrecht)

Die langfristige Verfügbarkeit des Vorgangs wird nicht über das Empfängerpostfach, sondern über die behördliche Aktenführung und das Archivrecht sichergestellt. Nach § 6a EGovG sollen die Behörden des Bundes ihre Akten elektronisch führen und dabei die Grundsätze ordnungsgemäßer Aktenführung nach dem Stand der Technik einhalten. Für die spätere Sicherung gelten die Anbietungs- und Aussonderungspflichten des Bundesarchivgesetzes: Unterlagen, die zur Aufgabenerfüllung nicht mehr benötigt werden und deren weitere Aufbewahrung nicht gestattet ist, sind dem Bundesarchiv anzubieten (§ 5 Abs. 1 BArchG), spätestens 30 Jahre nach Entstehung (§ 5 Abs. 1 Satz 2 BArchG); für geheimhaltungsbedürftige Unterlagen tritt § 6 BArchG hinzu.

Somit weist das Gesetz die Verantwortung für die langfristige, revisionssichere Vorhaltung der behördlichen Seite zu. Das Postfach ist demgegenüber Transport- und Zustellkanal. Eine langfristige Vorhaltung im Nutzerpostfach ist rechtlich weder zur Wirksamkeit der Bekanntgabe noch zur behördlichen Dokumentation erforderlich.

2.4. Datenschutzrechtliche Grenzen einer Dauervorhaltung

Umgekehrt bestehen datenschutzrechtliche Grenzen gegen eine unbegrenzte Vorhaltung. Personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO) und dürfen nur so lange in personenbezogener Form gespeichert werden, wie es für die Verarbeitungszwecke erforderlich ist (Speicherbegrenzung, Art. 5 Abs. 1 lit. e DSGVO). Eine dauerhafte Vorhaltung im Postfach „auf Vorrat" bedarf daher eines tragfähigen Zwecks und einer Rechtsgrundlage; sie ist im Zweifel durch Löschung bzw. eine bewusste, begründete Vorhaltefrist zu ersetzen. Die Ausgestaltung der Vorhaltedauer ist damit nicht frei, sondern datenschutzrechtlich zu rechtfertigen und minimierend zu gestalten.

2.5. Telekommunikations-/Verkehrsdatenrecht

Soweit der Betrieb der Postfachinfrastruktur der Sache nach Telekommunikationsdienste umfasst, gilt für Verkehrsdaten ein strenges Regime: Sie dürfen nur zu den in § 9 Abs. 1 TDDDG genannten Zwecken verarbeitet werden und sind im Übrigen nach Beendigung der Verbindung unverzüglich zu löschen (§ 9 Abs. 1 Satz 2 TDDDG). Eine darüberhinausgehende Verarbeitung ist unzulässig (§ 9 Abs. 1 Satz 3 TDDDG). Klar zu trennen ist dies von den Nachrichteninhalten im Postfach: Für deren Vorhaltung ist nicht § 9 TDDDG, sondern das allgemeine Datenschutzrecht (Art. 5 DSGVO, siehe D.III.1.) maßgeblich. Für die Architekturentscheidung folgt daraus, Verkehrsdaten und Inhaltsdaten getrennt zu behandeln und mit jeweils eigenen, gesetzeskonformen Löschregimen zu versehen.

2.6. Punktuelle Mindestvorhaltungspflichten als Referenzmodell (De-Mail-Gesetz)

Das De-Mail-G kennt zwar ebenfalls keine allgemeine Pflicht zur langfristigen Bereitstellung, enthält aber punktuelle Mindestvorhaltungs- bzw. Schutzregelungen zugunsten der Nutzer, die als Referenz für eine interessengerechte Ausgestaltung dienen können:

- Löschungsschutz nach Zustellung/Eingang: Nachrichten, für die eine Eingangs- oder Abholbestätigung erteilt wurde, können ohne sichere Anmeldung „erst 90 Tage nach ihrem Eingang gelöscht werden" (§ 5 Abs. 10 De-Mail-G). Dies ist dogmatisch kein Vorhalteanspruch, sondern ein Löschungsschutz zugunsten des Empfängers.

- Einstellung der Tätigkeit: Übernimmt kein anderer Anbieter das Konto, müssen die im Postfach und in der Dokumentenablage gespeicherten Daten „für wenigstens drei Monate ab dem Zeitpunkt der Benachrichtigung des Nutzers abrufbar bleiben" (§ 11 Abs. 2 De-Mail-G).

- Vertragsbeendigung: Dem Nutzer ist „für einen Zeitraum von drei Monaten nach Vertragsende" der Zugriff auf die abgelegten Daten zu ermöglichen, verbunden mit einem Löschhinweis mindestens einen Monat vorher (§ 12 De-Mail-G).

Diese Regelungen belegen, dass der Gesetzgeber bei Beendigungs- und Übergangskonstellationen ein berechtigtes Kontinuitäts- und Sicherungsinteresse der Nutzer anerkennt und über befristete Mindest-Abrufmöglichkeiten absichert – ohne daraus eine unbefristete Vorhaltung zu machen.

2.7. Folgerungen für die Architektur von ZaPuK

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Keine gesetzliche Dauervorhaltepflicht: Eine langfristige Bereitstellung abgerufener Nachrichten im zentralen Postfach ist rechtlich nicht geboten. Die Wirksamkeit einer Bekanntgabe hängt nicht von einer fortdauernden Präsenz der Nachricht im Postfach ab (§ 9 OZG; § 41 Abs. 2a VwVfG; § 122a AO; § 37 Abs. 2a SGB X).

- Speicherbarkeit statt Vorhaltung: Architektonisch genügt und geboten ist, dass Nutzer abgerufene Dokumente selbst speichern/exportieren können (so ausdrücklich § 9 Abs. 1 Satz 3 OZG; § 41 Abs. 2a Satz 2 VwVfG). Eine niederschwellige Export-/Download-Funktion sollte daher zwingend vorgesehen werden.

- Dokumentation behördenseitig: Die revisionssichere Langzeitsicherung erfolgt über die (elektronische) Aktenführung und das Archivrecht der jeweils zuständigen Stelle (§ 6a EGovG; §§ 5, 6 BArchG), nicht über das Empfängerpostfach.

- Definierte, begründete Vorhaltefristen: Die Vorhaltedauer im Postfach ist als Gestaltungsentscheidung (Nutzungsbedingungen/Rechtsgrundlage) festzulegen und am Maßstab von Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 lit. c und e DSGVO) auszurichten; Verkehrsdaten sind hiervon getrennt und nach § 9 TDDDG zu behandeln.

- Interessengerechte Mindestabsicherung: Als Orientierung für nutzerfreundliche Übergangs- und Beendigungsregeln (Kontoauflösung, Anbieter-/Systemwechsel, Löschung) bieten sich die De-Mail-Wertungen an: befristeter Löschungsschutz nach Zugang, mehrmonatige Abruf-/Zugriffsmöglichkeit bei Beendigung und vorherige Löschhinweise (§ 5 Abs. 10, § 11 Abs. 2, § 12 De-Mail-G).

Anregung *de lege ferenda*: Da ZaPuK bestehende Lösungen kanalübergreifend (Verwaltung und Justiz) ablösen soll, empfiehlt sich eine ausdrückliche gesetzliche Regelung der Vorhalte-, Export- und Löschmodalitäten des zentralen Postfachs, um Rechtssicherheit für Bekanntgabe-/Zustellwirkungen, Datenschutz und Nutzererwartungen einheitlich herzustellen.

3. Anschlussbedingungen und Föderationskontrolle

Kurzzusammenfassung. Die Zielarchitektur steuert die Teilnahme am Kommunikationsverbund über Anschlussbedingungen, deren Einhaltung risikobasiert zugesichert und über die Föderationsliste durchgesetzt wird (ADR-1145). Dieser Ansatz ist rechtlich tragfähig, sollte aber in zweifacher Hinsicht ergänzt werden.

Erstens sind Anschlussbedingungen ihrer Rechtsnatur nach vertragliche Regelungen und wirken deshalb nur zwischen den Vertragsparteien. Sie können weder Bindungswirkung gegenüber Ländern und Kommunen erzeugen, die sich dem Verbund nicht anschließen, noch Drittwirkung zugunsten oder zulasten der Kommunikationsteilnehmenden entfalten, noch die Anerkennung von ZaPuK als sicherer Übermittlungsweg oder als qualifizierter Zustelldienst ersetzen. Das Verbindungsnetz nach § 4 Abs. 1 Nr. 4 IT-NetzG zeigt, dass sich dies durch die Kombination eines vom IT-Planungsrat beschlossenen, fortschreibbaren Regelwerks mit einem individuellen Anschlussvertrag auflösen lässt.

Zweitens bewegt sich ZaPuK in einem bereits vorhandenen Regelungsrahmen. Für IT-Komponenten des Portalverbunds gilt die ITSiV-PV unmittelbar, und § 2 Abs. 6 Satz 2 ITSiV-PV nennt das Postfach ausdrücklich als Komponente, die vor Anbindung einem Penetrationstest und einem Webcheck zu unterziehen ist. Ein erheblicher Teil dessen, was ADR-1145 für eine vertragliche Regelung vorsieht, ist damit bereits verordnungsrechtlich vorgegeben. Die Anschlussbedingungen sollten dies aufnehmen, statt es zu duplizieren oder zu unterschreiten.

Empfohlen wird eine gestufte Regelungsarchitektur: Rechtsverordnung und Beschluss des IT-Planungsrats dort, wo Verbindlichkeit gegenüber Verwaltungsträgern oder Wirkung gegenüber Dritten erforderlich ist; vertraglicher Beitritt zu einem gemeinsam beschlossenen Regelwerk für alles Übrige, insbesondere für private Betreiber und für die Haftungszuordnung.

3.1. Ansatz von ZaPuK

ADR-1145 verwirft eine vollständige Zertifizierung und laufende Auditierung anzuschließender Postfach-Backends und entscheidet sich für eine risikobasierte Durchsetzung. Jede einzelne Anschlussbedingung wird danach eingeordnet, welcher Schaden bei Nichteinhaltung entsteht und ob ein Verstoß überhaupt feststellbar ist. Unterschieden werden fünf Zusicherungsarten: strukturell begrenzte Bedingungen, technisch geprüfte Bedingungen, nachträglich erkennbare Bedingungen, rein vertraglich abgesicherte Bedingungen sowie – als Ausnahme – die anlassbezogene oder stichprobenartige Konformitätsprüfung.

Adressiert werden zwei Rollen: der Betreiber eines Postfach-Backends und die anschließende Organisation, in deren Machtbereich Fachverfahren, Berechtigungsverzeichnis, Raum-Management-Service, Org-IdP-Adapter und E2EE-Endpunkte liegen. Im souveränen Betriebsmodell fallen beide Rollen zusammen. Postfachzugänge (Clients) unterliegen bewusst keiner Zulassung (ADR-0003). Beide Rollen nehmen den Anschlussvertrag im Onboarding des Self-Service-Portals (SSP) an (ADR-0008). Aufnahme, Suspendierung und Ausschluss werden über die Föderationsliste gesteuert. Deren Beachtung ist ihrerseits Anschlussbedingung, sodass die Durchsetzung wesentlich auf Gegenseitigkeit beruht.

Dieses Muster ist nicht neu. Die FITKO verwendet für die Anbindung an FIT-Connect bereits veröffentlichte Nutzungsbedingungen für die Produktivumgebung, die Rechte und Pflichten der anschließenden Stellen regeln und über die auch inhaltliche Vorgaben – etwa zur maschinenlesbaren Übermittlung – verbindlich gemacht werden. Da die zentralen Backend-Komponenten nach dem Betriebszielbild im Produkt FIT-Connect verortet werden sollen, kommt eine Fortschreibung dieses bestehenden Regelwerks in Betracht anstelle eines eigenständigen ZaPuK-Vertragswerks.

3.2. Rechtsnatur

3.2.1. Anschlussbedingungen als vertragliche Regelung und AGB

Die ZaPuK-Anschlussbedingungen begründen ein Rechtsverhältnis zwischen dem Betreiber der zentralen Infrastruktur und der anschließenden Stelle. Sie sind für eine Vielzahl von Anschlussfällen vorformuliert und werden im Onboarding einseitig gestellt; es handelt sich also um Allgemeine Geschäftsbedingungen im Sinne des § 305 Abs. 1 BGB.

a) Öffentlich-rechtliche oder privatrechtliche Ausgestaltung

Vorgelagert ist die Frage nach der Rechtsnatur. Beim Anschluss öffentlicher Stellen an eine gemeinsam getragene Verwaltungsinfrastruktur liegt ein öffentlich-rechtlicher Vertrag nach § 54 VwVfG nahe. Bei privaten Organisationen spricht viel für eine privatrechtliche Ausgestaltung. Im ersten Fall sind die §§ 305 ff. BGB über § 62 Satz 2 VwVfG entsprechend heranzuziehen, im zweiten gelten sie unmittelbar. Die Wahl ist nicht beliebig, sondern richtet sich nach dem

Gegenstand des Vertrags. Sie sollte bewusst getroffen und begründet werden. Denkbar ist auch eine Aufteilung nach Teilnehmergruppen.

Praktisch bedeutsam ist in beiden Fällen § 310 Abs. 1 BGB: Gegenüber Unternehmern und juristischen Personen des öffentlichen Rechts sind die Klauselverbote der §§ 308, 309 BGB nicht anwendbar, die Inhaltskontrolle nach § 307 Abs. 1 und 2 BGB bleibt jedoch eröffnet. Für die Gestaltung folgt daraus vor allem eine Anforderung an Änderungsklauseln. Anschlussbedingungen einer sich technisch fortentwickelnden Infrastruktur müssen dynamisch fortschreibbar sein; ein unbeschränkter einseitiger Änderungsvorbehalt hielte einer Kontrolle am Maßstab des § 307 BGB aber nicht stand. Erforderlich sind daher ein bestimmter Änderungsanlass, angemessene Übergangsfristen und ein Lösungsrecht der Gegenseite.

b) Schriftformerfordernis

Wird der Vertrag öffentlich-rechtlich geschlossen, ist er nach § 57 VwVfG schriftlich zu schließen, soweit nicht durch Rechtsvorschrift eine andere Form vorgeschrieben ist. Schriftform bedeutet die eigenhändige Unterzeichnung durch beide Parteien auf derselben Urkunde (§ 62 Satz 2 VwVfG iVm § 126 Abs. 1 und 2 BGB). Ein rein klickbasiertes Onboarding im SSP würde der Schriftform nicht genügen. Ein Formmangel führt im Übrigen nach zur Nichtigkeit (§ 59 Abs. 1 VwVfG iVm § 125 Satz 1 BGB), sodass die Grundlage der vertraglichen Zusicherungen entfallen würde, auf die das Durchsetzungskonzept nach ADR-1145 aufbaut.

Für eine Verwaltungsvereinbarung zwischen Verwaltungsträgern würde dasselbe gelten, denn auch sie ist ein öffentlich-rechtlicher Vertrag und unterliegt § 57 VwVfG. Sie bindet ebenso nur die Beteiligten.

c) Wege zur Formwahrung

Drei Gestaltungen kommen in Betracht. Erstens die qualifizierte elektronische Signatur beider Seiten nach § 3a Abs. 2 Satz 2 VwVfG beziehungsweise § 126a BGB. Sie ist rechtssicher, aber kaum praxistauglich für ein Massen-Onboarding. Zweitens – und vorzugswürdig – die Schriftformersetzung nach § 3a Abs. 3 VwVfG: teilnehmerseitig durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular mit elektronischem Identitätsnachweis (Nr. 1) oder

durch Übermittlung aus einem elektronischen Postfach, das nach einem Identifizierungsverfahren eingerichtet wurde (Nr. 2), betreiberseitig durch qualifiziertes elektronisches Siegel (Nr. 3). Dieser Weg lässt sich mit den ohnehin vorgesehenen Identifizierungsmitteln – BundID, Organisationskonto, perspektivisch EUDI-Wallet und European Business Wallet – unmittelbar im SSP abbilden. Drittens die privatrechtliche Ausgestaltung, die § 57 VwVfG (Schriftformerfordernis beim öffentlich-rechtlichen Vertrag) von vornherein nicht auslöst, aber wie dargestellt gesondert zu begründen wäre (siehe a)).

Ab dem 1. Juli 2027 vereinfacht sich die Lage durch die Neufassung des § 3a VwVfG und den neuen § 3b VwVfG (Art. 1 Nr. 3 des Gesetzes für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 3. Juli 2026). Nach § 3a Abs. 2 VwVfG n.F. wahrt ein elektronisches Dokument eine durch Rechtsvorschrift angeordnete Schriftform, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist. Ob diese Erleichterung auch § 57 VwVfG (Schriftformerfordernis beim öffentlich-rechtlichen Vertrag) erfasst oder ob dieser als eigenständige Formanordnung vorgeht, ist noch nicht geklärt und sollte vorab geprüft werden.

3.2.2. Vergleich: Anschlussbedingungen für das Verbindungsnetz

Nach § 4 Abs. 1 Nr. 4 IT-NetzG beschließen Bund und Länder gemeinsam im Koordinierungsgremium – dessen Aufgaben nach § 3 IT-StV der IT-Planungsrat wahrnimmt – die Anschlussbedingungen für das Verbindungsnetz, daneben die vom Netz zu erfüllenden Anforderungen, die Anschlussklassen, das Minimum anzubietender Dienste sowie die Anschlusskosten und deren Ermittlung. Die Beschlüsse kommen nach § 4 Abs. 3 IT-NetzG mit Zustimmung des Bundes und einer Mehrheit von elf Ländern zustande, die mindestens zwei Drittel der Finanzierungsanteile nach dem Königsteiner Schlüssel abbildet. Betrieben wird das Netz nach § 6 Abs. 1 IT-NetzG vom Bund, der nach § 5 Abs. 1 Satz 2 IT-NetzG Unternehmen mit Aufbau und Betrieb beauftragen kann.

a) Zweistufigkeit von Regelwerk und Einzelvertrag

Die Anschlussbedingungen wirken nicht unmittelbar, sondern werden als Anlage 3 in eine individuelle Leistungsvereinbarung zwischen dem Teilnehmer und der BDBOS als

Auftragnehmerin einbezogen; hinzu tritt eine Anlage 4 „E-Government durch Private bei Mehrfachnutzung".[405] Die Leistungsvereinbarung ordnet in Ziffer 1.2 eine ausdrückliche Rangfolge zwischen Hauptvertrag und Anlagen an. Dieses Modell bietet sich auch für ZaPuK an: kollektive Festlegung des Regelwerks im Gremium, individueller vertraglicher Beitritt im Einzelfall. Es löst das Legitimations- und das Änderungsproblem, denn die Fortschreibung geschieht durch Gremienbeschluss und nicht durch einseitigen Vorbehalt des Verwenders. Konsequent lässt Ziffer 11.3 der Leistungsvereinbarung Änderungen der Anlagen auch in elektronischer Form zu, während der Hauptvertrag der Schriftform unterliegt.

b) Öffnung für Private

Das Gesetz selbst adressiert Bund und Länder sowie „gegebenenfalls angeschlossene weitere öffentliche Stellen" (§ 7 Abs. 2 IT-NetzG). Die Öffnung für Private erfolgt erst auf der Ebene der Anschlussbedingungen: Private Dienstleister sind nach den Voraussetzungen des Kapitels 9, sechster Spiegelstrich der Anschlussbedingungen an das NdB-Verbindungsnetz angeschlossen, und die Leistungsvereinbarung verpflichtet den Teilnehmer in Ziffer 6.2 ausdrücklich, „soweit zutreffend" auch die Bedingungen der Anlage 4 zur Mehrfachnutzung durch Private einzuhalten. Für Private folgt die Bindung damit nicht aus dem IT-NetzG, sondern aus dem gremiengetragenen Regelwerk und der darauf gestützten vertraglichen Beziehung. Hinzu kommt, dass auch der Betrieb selbst privatwirtschaftlich erbracht wird – die BDBOS hat die Deutsche Telekom Business Solutions GmbH mit den Betriebsleistungen und dem Anschluss von Teilnehmern beauftragt, ohne dass diese Vertragspartei der Leistungsvereinbarung würde.

3.2.3. Durchsetzung ohne Zulassungsverfahren

Eine Zulassung oder Zertifizierung der Teilnehmer als Voraussetzung des Anschlusses sieht das Modell nicht vor. An ihre Stelle tritt eine Selbstverpflichtung, flankiert von einer vertraglichen Auskunftspflicht: Die Auftragnehmerin darf nach Ziffer 6.2 jederzeit Auskünfte über die Einhaltung der Anschlussbedingungen verlangen, der Teilnehmer muss binnen zwei Wochen antworten. Das entspricht strukturell exakt der in ADR-1145 gewählten Kombination aus

[405] Vgl. BDBOS, Leistungsvereinbarung Bundeseinrichtungen zum Anschluss an das NdB-Verbindungsnetz, Version 2.0.2.

vertraglicher Zusicherung und anlassbezogener Konformitätsprüfung. Technisch geprüft wird lediglich der Anschluss selbst, über ein Verfahren aus Betriebsbereitschaftserklärung, Prüfung der Funktionsfähigkeit und – bei Untätigkeit – Bestätigungsfiktion nach 28 Kalendertagen (Ziffer 4). Materiell verweisen die Anschlussbedingungen in ihrer aktuellen Fassung[406] auf ein eigenes IT-Grundschutzprofil. Ein IT-Grundschutzprofil ist nach der Terminologie des BSI ein Muster für Sicherheitskonzepte, also eine Vorlage für das ISMS des Teilnehmers, und begründet für sich genommen keine Zertifizierungspflicht.[407]

3.2.4. Ausschlussverfahren

Für den Fall, dass die Anschlussbedingungen nicht mehr erfüllt sind oder Auskünfte nicht fristgerecht erteilt werden, sieht Ziffer 10.3 der Leistungsvereinbarung ein Sonderkündigungsrecht mit einem gestuften Verfahren vor: Aufforderung zur Stellungnahme binnen 14 Tagen unter Ankündigung einer Abmahnung, sodann Abmahnung durch die Behördenleitung oder deren Vertretung mit einmonatiger Frist zur Beseitigung, schließlich Kündigung mit viermonatiger Frist, und zwar ausdrücklich im Einvernehmen mit dem Arbeitsgremium Verbindungsnetz. Die gesamte Kommunikation bedarf mindestens der Textform. Damit sind Anhörung, Eskalationsstufen, Fristen und Gremienbeteiligung geregelt. Dies entspricht den Punkten, die ADR-1145 für Suspendierung und Ausschluss aus der Föderationsliste noch offenlässt, und kann Vorbild sein.

3.2.5. Haftung und Sanktionen

Die Leistungsvereinbarung arbeitet mit einem Durchleitungsmodell: Vertragsstrafen aus dem Service Level Agreement und Schadensersatzansprüche gegen den privaten Betreiber werden von der Auftragnehmerin an den Teilnehmer weitergegeben, begrenzt auf die Höhe der Haftungsbegrenzung im Verhältnis zum Betreiber (Ziffern 3.2 bis 3.5, 9.1). Die Auftragnehmerin haftet also nicht originär, sondern reicht die Haftung durch. Die für den Teilnehmer

[406] Version 2.0.2 nach Beschluss 2020/15, angepasst durch Beschluss 2022/53.

[407] Ob die Anschlussbedingungen darüber hinaus einen förmlichen Sicherheitsnachweis verlangen, lässt sich ohne den Volltext des Regelwerks nicht abschließend beurteilen. Der Text ist nicht öffentlich verfügbar.

maßgebliche Haftungsobergrenze entsteht damit nicht in der Leistungsvereinbarung, sondern bereits im Beschaffungsvertrag zwischen Auftragnehmerin und Betreiber, also in einem Vertrag, an dem der Teilnehmer nicht beteiligt ist. Konsequent beziffert die Leistungsvereinbarung die Beträge in Ziffer 9.2 und benennt in Ziffer 9.3 die zwingenden Haftungsausnahmen. Für ZaPuK ist dieses mögliche Vorbild relevant, weil auch dort der Betrieb zentraler Komponenten an Dienstleister vergeben werden dürfte.

3.2.6. Verbleibende Unterschiede

Erstens beruhen die Anschlussbedingungen des Verbindungsnetzes auf einer ausdrücklichen verfassungsrechtlichen und einfachgesetzlichen Grundlage (Art. 91c Abs. 4 GG, IT-NetzG). An einer entsprechenden Grundlage fehlt es für ZaPuK. Zweitens betrifft das Verbindungsnetz die Netzebene und damit einen Transportkanal zwischen Verwaltungsnetzen, während ZaPuK die Anwendungsebene und die Rechtswirkungen einzelner Übermittlungen gegenüber Bürgerinnen, Bürgern und Unternehmen betrifft; die Anschlussbedingungen tragen dort eine deutlich größere rechtliche Last. Drittens ist der Teilnehmerkreis des Verbindungsnetzes trotz der Öffnung für Private überschaubar und institutionell gefiltert, während ZaPuK auf eine breite Beteiligung privater Organisationen angelegt ist (ADR-0004). Das erhöht die Anforderungen an Skalierbarkeit und Formtauglichkeit des Onboardings.

3.3. Weitere Vergleichsmodelle

Am strengsten ist das Zulassungsmodell der Telematikinfrastruktur: Nach § 325 Abs. 1 SGB V bedürfen Komponenten und Dienste der Zulassung durch die gematik, die auf Antrag erteilt und mit Nebenbestimmungen versehen werden kann. Die Prüfung erfolgt anhand veröffentlichter Prüfkriterien, der Sicherheitsnachweis nach im Benehmen mit dem BSI entwickelten Vorgaben (§ 325 Abs. 3 SGB V). Ähnlich lag das Akkreditierungsmodell des De-Mail-G. Beide Modelle erzeugen hohe Eintrittshürden. Im Fall von De-Mail hat dies ggf. die begrenzte Verbreitung mitverursacht, jedenfalls wird dieses Vorgehen mit dem Außerkrafttreten des De-Mail-G

zum Ablauf des 31. Dezember 2026 aufgegeben.[408] Die Entscheidung in ADR-1145 gegen eine Zertifizierungspflicht erscheint vor diesem Hintergrund gut begründet.

Ein Mittelweg findet sich in § 6 Abs. 1 ERVV für das besondere elektronische Behördenpostfach: Dort sind die Anschlussanforderungen – Protokollstandard nach dem Stand der Technik, geprüfte und bestätigte Identität des Postfachinhabers, Eintrag in ein sicheres Verzeichnis, Feststellbarkeit des Absenders – nicht vertraglich, sondern durch Rechtsverordnung festgelegt. Diese Struktur greift der künftige § 3c Abs. 1 VwVfG auf, der sichere Übermittlungswege an einen dem Stand der Technik entsprechenden Protokollstandard, die Feststellung der Identität der erklärenden Person und deren Authentisierung bindet und die Festlegung im Übrigen nach § 3c Abs. 2 VwVfG einer Rechtsverordnung des Bundesministeriums des Innern im Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung überantwortet.

3.4. Untergesetzliche und verordnungsrechtliche Verbindlichkeit

Für Standards, die gegenüber Bund und Ländern verbindlich sein sollen, steht die Beschlusskompetenz des IT-Planungsrats nach § 1 Abs. 1 Satz 1 Nr. 2 in Verbindung mit § 2 IT-StV zur Verfügung. Solche Beschlüsse entfalten nach § 2 Abs. 2 Satz 2 IT-StV ausdrücklich Bindungswirkung und sind innerhalb festzusetzender Fristen umzusetzen. Die Umsetzung im Bund richtet sich nach § 10 EGovG, in den Ländern nach den entsprechenden Landesregelungen (etwa § 20 EGovG NRW).

Noch weiter reichen die Verordnungsermächtigungen des OZG. Nach § 5 OZG werden die IT-Sicherheitsstandards für die im Portalverbund und zur Anbindung genutzten IT-Komponenten durch Rechtsverordnung festgelegt. Ihre Einhaltung ist für alle Stellen verbindlich, die entsprechende IT-Komponenten nutzen, und abweichendes Landesrecht ist ausgeschlossen. Die auf dieser Grundlage erlassene ITSiV-PV verlangt in § 2 Abs. 1 Maßnahmen nach dem Stand der Technik und knüpft daran in § 2 Abs. 2 eine Vermutungsregel bei Einhaltung der in der Anlage benannten Technischen Richtlinien des BSI. Dieses Modell dynamischer Verweisung lässt sich für die technischen Teile der ZaPuK-Anschlussbedingungen unmittelbar übertragen.

[408] Art. 4 Nr. 2 des Gesetzes vom 3. Juli 2026, BGBl. 2026 I Nr. 199.

Parallel dazu ermächtigt § 6 Abs. 1 OZG das BMI im Einvernehmen mit dem IT-Planungsrat, Architekturvorgaben, Qualitätsanforderungen und Interoperabilitätsstandards einschließlich Datenformaten, Transportprotokollen und Schnittstellenbeschreibungen festzulegen. Auch diese Vorgaben sind nach § 6 Abs. 3 OZG für alle Stellen verbindlich, deren Verwaltungsleistungen über den Portalverbund angeboten werden.

3.5. Funktion und Grenzen

Die Anschlussbedingungen erfüllen im Verbund vier Funktionen. Sie konstituieren den Vertrauensverbund, indem sie die Aufnahme in die Föderationsliste an überprüfbare Voraussetzungen knüpfen. Sie kompensieren Schutzziele, die technisch nicht erzwingbar sind – die Terminierung der Ende-zu-Ende-Verschlüsselung im eigenen Machtbereich, das Verbot der zweckwidrigen Auswertung und der domänenübergreifenden Zusammenführung von Metadaten, die Meldung von Sicherheitsvorfällen sowie das Verhalten der Org-IdP-Adapter. Sie schaffen eine Zurechnungs- und Haftungsgrundlage gegenüber einem bekannten, rechtlich belangbaren Betreiber. Und sie tragen mittelbar die Beweiswirkung der im Verbund erzeugten Nachweise: Eine Bereitstellungsbestätigung eines fremden Backends ist nur so belastbar wie die Zusicherung, unter der dieses Backend betrieben wird.

Aus der Rechtsnatur ergeben sich auch Grenzen dessen, was Anschlussbedingungen leisten können. Erstens wirken vertragliche Zusicherungen nur zwischen den Parteien. Bürgerinnen und Bürger können aus ihnen keine Rechte herleiten, und im Streit über den Zugang eines Verwaltungsakts hilft der Anschlussvertrag der Behörde allenfalls mittelbar. Zweitens lassen sich Verwaltungsträger, die dem Verbund nicht beitreten, vertraglich nicht binden. Für Verbindlichkeit gegenüber Ländern und Kommunen, wäre ein Beschluss nach § 2 IT-StV oder eine Rechtsverordnung nach §§ 5, 6 OZG notwendig. Für den Bereich der Justiz ist zusätzlich zu berücksichtigen, dass die Justizverwaltungen ihre IT-Standardsetzung bewusst im E-Justice-Rat gebündelt haben. Für auch insoweit wirksame Anschlussbedingungen müsste Einvernehmen hergestellt werden. Drittens ersetzen Anschlussbedingungen keine statusbegründende Rechtsgrundlage: Die Anerkennung von ZaPuK als sicherer Übermittlungsweg setzt nach künftigem Recht die Festlegung durch Rechtsverordnung nach § 3c Abs. 2 VwVfG voraus, und die

Vermutungswirkung eines qualifizierten Zustelldienstes nach Art. 43 Abs. 2 eIDAS-VO hängt an den Anforderungen des Art. 44 eIDAS-VO und am Status als qualifizierter Vertrauensdiensteanbieter, nicht an einer vertraglichen Selbstverpflichtung. Viertens dürfen die Anschlussbedingungen die verordnungsrechtlichen Vorgaben der ITSiV-PV weder unterschreiten noch abbedingen; sie können sie nur konkretisieren, auf nicht erfasste Teilnehmergruppen erstrecken und ihre Nachweisführung organisieren. Fünftens teilen die Anschlussbedingungen das Schicksal des Vertrags, in den sie einbezogen sind, und hängen insoweit von der Einhaltung der Form ab (dazu 3.2.1). Sechstens ist der Ausschluss eines Betreibers aus der Föderationsliste ein erheblicher Eingriff in dessen Rechtsposition. Voraussetzungen, Zuständigkeit, Anhörung und Rechtsschutz müssen deshalb im Vertragswerk selbst hinreichend bestimmt geregelt sein. ADR-1145 weist dies zu Recht als offenen Punkt aus.

3.6. Zu regelnde Punkte

Die hier entwickelten Empfehlungen laufen an mehreren Stellen auf Festlegungen hinaus, die in den Anschlussbedingungen zu verankern sind. Zusammengefasst betrifft dies:

- Metadatenschutz und Betreiberausschluss: ausdrückliche Zusammenführungs- und Querzugriffsverbote für Metadaten zwischen Bürger- und Organisationsdomäne, Spiegelung der Klauseln bei Unterauftragsverhältnissen, Offenlegungspflicht bei unzulässigen Weisungen sowie Change-Control-Klauseln, die eine spätere Aufweichung dieser Vorgaben ausschließen oder an enge Voraussetzungen binden (vgl. III.3.6.3; ADR-1105, ADR-1106).

- Datenschutzrechtliche Rollen: Festlegung von getrennter oder gemeinsamer Verantwortlichkeit, Vereinbarungen nach Art. 26 bzw. Art. 28 DSGVO; soweit möglich, ergänzende Klarstellung durch Rechtsvorschrift (vgl. III.2.2).

- Integrität und Kryptographie: kryptographische Integritätssicherung nach dem Stand der Technik, dokumentiertes Kryptokonzept, Schlüssellebenszyklus, Hardware-Sicherheitsmodule für Signaturschlüssel, Krypto-Agilität und Vorhaltung historischer Prüfschlüssel für die Langzeitprüfbarkeit (vgl. III.3.6.1; III.3.6.2; ADR-1144).

- Nachweiserzeugung: verpflichtende Erzeugung signierter Bereitstellungsbestätigungen, Mindestumfang der Zustelloptionen, Bereitstellung des Upload-Endpunkts beziehungsweise der Schnittstelle des Medien-Prüfdienstes, qualifizierte Zeitstempel für beweiskritische Anwendungsfälle (vgl. III.3.6.1; III.5.7; ADR-0018, ADR-1119, ADR-1120).

- Schlüsselwiederherstellung: Pflicht zur Bereitstellung eines funktionsfähigen Wiederherstellungsverfahrens, da ohne sie trotz Bereitstellungsbestätigung mangelnder Zugang geltend gemacht werden kann (vgl. 1).

- Aufbewahrung, Löschung und Verfügbarkeit: Löschfristen für verschlüsselte Anhänge, Mindestvorhaltefristen im Postfach, Übergabepaket für Veraktung und Archivierung, Datenübergabe beim Austritt aus dem Verbund (vgl. III.3.5.1, 1; ADR-1135).

- Telekommunikationsrechtliche Pflichten: Zuordnung der Pflichten aus dem TDDDG, insbesondere zum Fernmeldegeheimnis und zur Behandlung von Verkehrsdaten, soweit einzelne Komponenten als nummernunabhängiger interpersoneller Telekommunikationsdienst einzuordnen sind (vgl. V).

- Betrieb und Vorfallmanagement: sicherer Betrieb nach dem Stand der Technik, Einbindung in ein ISMS, Meldepflichten bei Sicherheitsvorfällen, Verfügbarkeits- und Reaktionszeiten als Service-Level, Auskunftspflicht mit fester Antwortfrist.

- Verfahren: Voraussetzungen und Verfahren für Suspendierung und Ausschluss, Anhörung und Rechtsbehelf, Anlass und Umfang anlassbezogener Konformitätsprüfungen.

3.7. Empfehlungen und Ableitungen für die Architektur

Aus dem Vorstehenden ergibt sich für die Architektur von ZaPuK:

- Der risikobasierte Ansatz aus ADR-1145 erscheint rechtlich tragfähig und zielführend. Er entspricht dem beim Verbindungsnetz praktizierten Modell und ist einer Zertifizierung nach dem Vorbild des § 325 SGB V oder der De-Mail-Akkreditierung vorzuziehen, die dem Ziel eines niedrigschwelligen Anschlusses entgegenstünde.

- Für die Anschlussbedingungen ist ein dreistufiger rechtlicher Rahmen zu empfehlen: Rechtsverordnung nach §§ 5, 6 OZG für Architektur-, Interoperabilitäts- und Sicherheitsvorgaben mit Wirkung gegenüber allen Stellen; Beschluss des IT-Planungsrats nach § 2 IT-StV für die föderale Bindungswirkung dort, wo eine Verordnung nicht trägt; Anschlussvertrag im SSP409-Onboarding für die betreiberbezogenen Pflichten, die Haftung und die Föderationskontrolle. Die vertragliche Ebene sollte auf die Ebenen darüber verweisen, statt deren Inhalte zu duplizieren.

- Nach dem Vorbild des Verbindungsnetzes sollte das Regelwerk nicht vom Betreiber einseitig gestellt, sondern vom IT-Planungsrat beschlossen und im Einzelvertrag lediglich als Anlage in Bezug genommen werden. Der Vertrag sollte eine Rangfolge zwischen Hauptvertrag und Anlagen festlegen und die Fortschreibung der Anlagen erleichtert – insbesondere ohne Schriftform – zulassen. Das erhöht die Legitimation gegenüber den Ländern und entschärft zugleich die AGB-rechtliche Problematik einseitiger Änderungsvorbehalte.

- Für private Betreiber und IT-Dienstleister ist ein eigener Regelungsteil zu empfehlen, wie ihn das Verbindungsnetz mit Kapitel 9 der Anschlussbedingungen und der Anlage zur Mehrfachnutzung durch Private kennt (vgl. zur Öffnung für den unmittelbaren Anschluss privater ADR-0004).

- Zur Durchsetzung sollte an Stelle einer Prüfpflicht eine vertragliche Auskunftspflicht mit fester Frist erwogen werden, wie sie Ziffer 6.2 der Leistungsvereinbarung für das Verbindungsnetz mit zwei Wochen vorsieht. Damit wären die in ADR-1145 als vertraglich eingestuften Bedingungen bis zu einem gewissen Grad überprüfbar, ohne ein Auditregime aufzubauen.

- Für Suspendierung und Ausschluss aus der Föderationsliste kommt ein gestuftes Verfahren wie in Ziffer 10.3 der Leistungsvereinbarung für das Verbindungsnetz in Betracht: Aufforderung zur Stellungnahme, Abmahnung durch die Leitungsebene mit

[409] Self-Service-Portal.

Beseitigungsfrist, Kündigung im Einvernehmen mit einem Gremium des IT-Planungsrats, jeweils mindestens in Textform. Für den Verbund wäre ergänzend zu regeln, ab welchem Zeitpunkt die Suspendierung technisch in der Föderationsliste wirkt und binnen welcher Frist die angeschlossenen Backends sie umzusetzen haben.

- Rechtsnatur und Form der Anschlussbedingungen müssen festgelegt werden. Vorgelagert ist die Entscheidung, ob das Anschlussverhältnis öffentlich-rechtlich oder privatrechtlich ausgestaltet wird – gegebenenfalls unterschiedlich für öffentliche Stellen und private Organisationen. Nur bei öffentlich-rechtlicher Ausgestaltung greift das Schriftformgebot des § 57 VwVfG (auch im Falle einer Verwaltungsvereinbarung). Ein Formmangel ist zu vermeiden, da er zur Nichtigkeit führt (§ 59 Abs. 1 VwVfG iVm § 125 Satz 1 BGB). Insofern ist zu beachten, dass ein rein klickbasierter Abschluss im SSP der Schriftform nicht genügt. In Betracht zu ziehen ist die Schriftformersetzung nach § 3a Abs. 3 VwVfG, die sich mit den ohnehin vorgesehenen Identifizierungsmitteln (BundID, Organisationskonto, perspektivisch EUDI-Wallet) unmittelbar im SSP abbilden ließe. Eine privatrechtliche Ausgestaltung würde das Schriftformerfordernis des § 57 VwVfG gänzlich vermeiden. Ab dem 1. Juli 2027 vereinfacht sich die Lage durch § 3a Abs. 2 und § 3b VwVfG n.F. (ob die dortige Erleichterung auch § 57 VwVfG erfasst, wäre ggf. noch zu klären).

- Die mögliche Nichtigkeitsfolge bei Formmangel ist ein zusätzliches Argument für eine dreistufige Regelung. Sind die tragenden Pflichten in Rechtsverordnung und Beschluss des IT-Planungsrats verankert und nimmt der Anschlussvertrag sie lediglich in Bezug, bleiben sie auch dann bestehen, wenn der Einzelvertrag an einem Formmangel oder aus anderen Gründen scheitert. Die vertragliche Ebene sollte deshalb möglichst wenig eigenständig begründen und möglichst viel verweisen.

- Für die technischen Anforderungen kann die Verweistechnik des § 2 Abs. 2 ITSiV-PV Vorbild sein: Verweis auf benannte Spezifikationen und Technische Richtlinien mit Vermutungswirkung, Bekanntgabe der jeweils geltenden Fassung und Übergangsfrist bei Fortschreibung.

- Die Anerkennung als sicherer Übermittlungsweg ist frühzeitig über die Verordnung nach § 3c Abs. 2 VwVfG zu adressieren. Die Architektur erfüllt die materiellen Kriterien des § 3c Abs. 1 VwVfG bereits (Protokollstandard, Identitätsfeststellung, Authentisierung zur Übermittlung). Die Anschlussbedingungen sollten so formuliert werden, dass sie unmittelbar als Nachweis dieser Kriterien dienen können.

- Wo eine Beweiswirkung nach Art. 43 Abs. 2 eIDAS-VO angestrebt wird, ist die vertragliche Ebene nicht ausreichend. Der Status als qualifizierter Vertrauensdiensteanbieter sollte auf die zentralen Betreiber beziehungsweise einen dedizierten Quittungs- und Zeitstempeldienst gebündelt werden. Für souveräne Backends ohne diesen Status ist transparent zu machen, dass ihre Bereitstellungsbestätigungen nur die Wirkung des Art. 43 Abs. 1 eIDAS-VO entfalten.

- Bei Vergabe des Betriebs zentraler Komponenten an Dienstleister sollte für die Haftung das Durchleitungsmodell in Erwägung gezogen werden, wie es die Leistungsvereinbarung zum Verbindungsnetz in den Ziffern 3.2 bis 3.5 und 9.1 vorsieht: Der zentrale Betreiber gibt Vertragsstrafen und Schadensersatzansprüche gegen den Dienstleister an die angeschlossenen Stellen weiter. Die Haftungsobergrenze für den gesamten Verbund ergibt sich aus dem Beschaffungsvertrag zwischen zentralem Betreiber und Dienstleister und ist für die anschließende Stelle nicht verhandelbar. Die Durchleitungsklausel muss dem Transparenzgebot des § 307 Abs. 1 Satz 2 BGB genügen. Ein bloßer Verweis auf die Haftungsgrenze eines dem Teilnehmer unbekannten Vertrags dürfte nicht ausreichen, die Beträge und die zwingenden Haftungsausnahmen sind daher zu beziffern.

***

E. Möglichkeiten und Grenzen des IT-StV (Ergänzende Stellungnahme vom 19.10.2026)

I. Einleitung und Fragestellung

In verfassungsrechtlicher Hinsicht umfassen die Empfehlungen des Rechtsgutachtens unter anderem eine **staatsvertragliche Lösung auf Grundlage von Art. 91c Abs. 1 und 2 GG** zur übergreifenden Regelung des Zusammenwirkens in Bezug auf ZaPuK. Bei einem solchen Staatsvertrag kann es sich danach um einen neuen, eigenständigen Staatsvertrag für ZaPuK handeln, angesprochen ist aber ebenso die Möglichkeit, bereits vorhandene Regelungen und Strukturen, beispielsweise solche des IT-Staatsvertrags, als Ausgangspunkt für die Umsetzung von ZaPuK zu nutzen (siehe D.I.2.2.3.c) am Ende; vgl. auch die Ausführungen unter D.I.2.2.3.d) und D.I.2.3.).

Ausgehend hiervon soll in diesem Abschnitt E. ergänzend und vertiefend der Frage nachgegangen werden, inwieweit der bestehende IT-Staatsvertrag in seiner aktuellen Fassung für die Umsetzung von ZaPuK genutzt werden kann. Aufzuzeigen sind die rechtlichen Möglichkeiten und Grenzen des IT-Staatsvertrags im Hinblick auf einen Ansatz, nach dem ZaPuK (oder einzelne Komponenten von ZaPuK) als Produkt des IT-Planungsrats im Rahmen des Produktmanagements der FITKO bereitgestellt und finanziert wird.

II. Möglichkeiten: ZaPuK als Produkt des IT-Planungsrats

Der IT-Staatsvertrag wurde 2009 zwischen dem Bund und den Ländern als „Vertrag zur Ausführung von Artikel 91c GG" abgeschlossen. Mit ihm wurde auf Basis von Art. 91c Abs. 1 und 2 GG der IT-Planungsrat eingerichtet und diesem mit § 1 Abs. 1 IT-StV verschiedene Aufgaben im Bereich der IT-Zusammenarbeit zwischen Bund und Ländern zugewiesen. Im Zuge der Verstetigung und Bündelung der zunächst kurzfristig angelegten Projekte entwickelte sich ein Portfolio von inzwischen 15 Produkten, welches nunmehr mit Unterstützung der zum Jahr 2020 errichteten FITKO (vgl. § 5 Abs. 1 Satz 3 IT-StV) und nach einem einheitlichen, durch den IT-Planungsrat mit Beschluss B-2024/51-IT vom 13. November 2024 festgelegten Produktmanagement-Modell gesteuert wird.

Ein „Produkt" wird dabei verstanden als „eine dauerhafte Lösung für ein Problem aus dem Zuständigkeitsbereich des IT-Planungsrats", welches „für bestimmte Zielgruppen wie Bürger:innen, Verwaltungsmitarbeitende sowie Unternehmen und staatliche Institutionen nützlich ist. Die Produkte besitzen typischerweise Querschnittscharakter und richten sich an den strategischen Schwerpunktthemen des IT-Planungsrats aus."[410] Die konkrete Übernahme von Produkten in das Produktportfolio des IT-Planungsrats und das Produktmanagement durch die FITKO erfolgt jeweils durch Beschluss des IT-Planungsrats.[411]

Die rechtliche Grundlage für das Produktmanagement durch den IT-Planungsrat bzw. die FITKO ergibt sich aus § 1 Abs. 1 Satz 1 Nr. 3, 4 und 5 IT-StV, jeweils in Verbindung mit § 5 Abs. 1 Satz 3 IT-StV. Die Nr. 3 bis 5 beinhalten dabei jeweils verschiedene Kompetenzen im Zusammenhang mit der IT-Zusammenarbeit und Verwaltungsdigitalisierung, die zusammengenommen den gesamten Lebenszyklus eines Produkts von der Entwicklung über die Bereitstellung bis zu Steuerung und Betrieb desselben abbilden können.[412] Die vorgesehenen Aufgaben spiegeln insofern die verfassungsrechtliche Ermächtigungsgrundlage in Art. 91c Abs. 1 GG wieder, die die Möglichkeiten des Zusammenwirkens zwischen Bund und Ländern auf die Planung, die Errichtung und den Betrieb der für ihre Aufgabenerfüllung erforderlichen IT-Systeme erstreckt.[413]

Auf Grundlage von § 1 Abs. 1 Satz 1 Nr. 3, 4 und 5 IT-StV ist aus rechtlicher Sicht grundsätzlich auch vorstellbar, dass ZaPuK – als Ganzes[414] oder jedenfalls mit einem Teil seiner Komponenten wie der Postfach-Backends für Organisationen, dem Adressregister und dem Self-Service-Portal – von der FITKO entwickelt, bereitgestellt und betrieben wird: Die zentrale Norm des

[410] Gesamtdokumentation zu Beschluss B-2024/51-IT, Produktmanagement-Modell für die Produkte des IT-Planungsrats, Version 1.0, Stand: 30.09.2024, S. 4/5.
[411] Vgl. zum Beispiel Beschluss B-2022/32-IT vom 6. September 2022, mit dem FIT-Connect zum Produkt des IT-Planungsrats erklärt wurde.
[412] Für ein Beispiel der umfassenden Aufgabenübernahme bzgl. eines Produkts siehe den Beschluss B-2022/32-IT vom 6. September 2022 zu FIT-Connect. Betriebsverantwortung dürfte insbesondere in den Fällen bei der FITKO liegen, in denen das Steuerungsmodell „Owner" Anwendung findet, vgl. Gesamtdokumentation zu Beschluss B-2024/51-IT, Produktmanagement-Modell für die Produkte des IT-Planungsrats, Version 1.0, Stand: 30.09.2024, S. 15 ff.
[413] Siehe dazu bereits die Ausführungen unter D.I.2.2.3.
[414] Vorbehaltlich insb. datenschutzrechtlicher Erwägungen, vgl. dazu unter anderem D.III.1.3.2.c) und D.III.3.6.3 sowie Abschnitte 4.2.1 und 4.2.3.1 des Architekturkonzepts.

Produktmanagementmodells bildet dabei zunächst § 1 Abs. 1 Satz 1 Nr. 4 IT-StV[415], nach der die FITKO „Produkte des informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens" „steuert", die der IT-Planungsrat durch Beschluss in sein Produktportfolio aufnimmt.[416] Unter „Steuerung" werden üblicherweise eher Lenkungs- und Überwachungsaufgaben verstanden. Für die Entwicklung und Bereitstellung der erforderlichen Komponenten steht jedoch ergänzend § 1 Abs. 1 Nr. 5 IT-StV zur Verfügung, nach dem der IT-Planungsrat bzw. die FITKO „kurzfristig bund- und länderübergreifend einsetzbare digitale Lösungen für bestimmte Lebensbereiche zur Verfügung stellen oder projektieren" kann. Schließlich kann der FITKO auf Basis von § 1 Abs. 1 Satz 1 Nr. 3 IT-StV grundsätzlich auch die Verantwortung für den operativen Betrieb (ggf. durch von ihr beauftragte Dienstleister) von ZaPuK bzw. einzelner Komponenten des Kommunikationsverbunds übertragen werden. Denn danach kann der IT-Planungsrat solche Digitalisierungslösungen „betreiben lassen", die aus der „Zusammenarbeit von Bund und Ländern in Fragen der Digitalisierung von Verwaltungsleistungen" resultieren.

Zusammengefasst bietet der IT-Staatsvertrag in seiner aktuellen Fassung grundsätzlich die Möglichkeit, ZaPuK oder einen Teil der ZaPuK-Komponenten durch die FITKO bereitzustellen und im Rahmen des Produktmanagements betreiben zu lassen. Allerdings ist eine solche Lösung in ihrer Reichweite begrenzt (dazu sogleich unter **III.1. und 2.**) und muss gegebenenfalls durch zusätzliche Regelungen ergänzt werden (dazu **III.4. und 5.**). Darüber hinaus ergeben sich aus den zugrundeliegenden Rechtsgrundlagen des IT-Staatsvertrags sowie den verfassungsrechtlichen Grundlagen Grenzen im Hinblick auf die Möglichkeiten zur Finanzierung des Produkts (siehe dazu **III.3.**).

Durch zusätzliche staatsvertragliche Regelungen – ob in einem separaten ZaPuK-Staatsvertrag, als Teil eines D-Stack-Staatsvertrags oder als Erweiterung des IT-Staatsvertrags – können gegebenenfalls einige dieser Grenzen überwunden oder jedenfalls verschoben werden. Den

[415] § 1 Abs. 1 Nr. 4 IT-StV wird auf der Website des Produktmanagements der FITKO als Grundlage angegeben, https://www.fitko.de/produktmanagement, zuletzt abgerufen am 15.10.2026.
[416] Konkretisiert wird dieses Vorgehen im Rahmen des Produktmanagementmodells, vgl. Gesamtdokumentation zu Beschluss B-2024/51-IT, Produktmanagement-Modell für die Produkte des IT-Planungsrats, Version 1.0, Stand: 30.09.2024, S. 34/35.

insofern aus unserer Sicht bestehenden rechtlichen Mehrwert zusätzlicher staatsvertraglicher Regelungen haben wir abschließend unter **IV.** noch einmal zusammengefasst.

III. Grenzen

1. Verbindlichkeit

Allein über den IT-Staatsvertrag kann eine verbindliche Anschluss- und Nutzungsverpflichtung hinsichtlich des ZaPuK-Kommunikationsverbunds gegenüber den Ländern (einschließlich der Kommunen) bzw. dem Bund nicht hergestellt werden.

Soweit der IT-Planungsrat gemäß § 2 IT-StV Festlegungen hinsichtlich IT-Interoperabilitäts- und IT-Sicherheitsstandards trifft, sind diese Beschlüsse auf Basis von Art. 91c Abs. 2 GG zwar verbindlich. In § 2 Abs. 2 Satz 2 IT-StV wird insofern ausdrücklich darauf verwiesen, dass die Beschlüsse Bindungswirkung entfalten und von Bund und den Ländern innerhalb jeweils vom IT-Planungsrat festzusetzender Fristen in ihren jeweiligen Verwaltungsräumen umgesetzt werden. Für die in § 1 Abs. 1 Satz 1 Nr. 4 IT-StV adressierten Produkte ist jedoch keine vergleichbare Verbindlichkeit vorgesehen. Die Länder bzw. der Bund können an einem Produkt des IT-Planungsrats durch Beitrittserklärung teilnehmen.[417] Die Teilnahme ist freiwillig. Eine verbindliche Anschluss- und Nutzungsverpflichtung einzelner Komponenten von ZaPuK durch Bund und Länder – einschließlich der Kommunen – bedarf insofern einer anderen/weiteren Rechtsgrundlage.

2. Perspektivische Einbeziehung der Justiz

Bezüglich einer perspektivischen Einbeziehung der Justiz ist zu berücksichtigen, dass die informationstechnischen Systeme in der Justiz grundsätzlich nicht im Zuständigkeitsbereich des IT-Planungsrats liegen. Mit dem E-Justice-Rat existiert ein institutionell vorgesehenes „Partnergremium" des IT-Planungsrats, über das Bund und Länder ihre Zusammenarbeit gemäß Art. 91c Abs. 1 und 2 GG im Bereich der informationstechnischen Systeme der Justiz ausüben (siehe D.VI.1.). Hieraus entsteht aber kein grundsätzliches Hindernis für eine perspektivische

[417] Vgl. Ziffer 1 Abs. 1 und 2 Allgemeine Teilnahmebedingungen für die Produkte des IT-Planungsrats, Version: 1.0, Stand: 30.09.2024.

Anbindung des EGVP-Verbunds an den ZaPuK-Kommunikationsverbund bei einer Bereitstellung und Finanzierung einzelner ZaPuK-Komponenten als Produkt des IT-Planungsrats im Rahmen des Produktmanagements der FITKO, da eine Zusammenarbeit der von Bund und Ländern eingerichteten E-Justice-Gremien mit dem IT-Planungsrat vorgesehen ist.

Diese Zusammenarbeit wird auch in der Erklärung des IT-Planungsrats zu § 17 der Geschäftsordnung – siehe Beschluss B-2026/21-IT vom 17. Juni 2026 zur Geschäftsordnung des IT-Planungsrats – bekräftigt, in der die Fortsetzung der Kooperation zwischen E-Government und E-Justice unter Wahrung der besonderen Anforderungen der Justiz ausdrücklich vorgesehen ist:

> „1. E-Justice und E-Government haben sich in den vergangenen Jahren in enger Kooperation positiv entwickelt. Es ist Ziel des IT-Planungsrats, diese Zusammenarbeit und gemeinsame Entwicklung fortzusetzen und bei der Steuerung des E-Government mit den von Bund und Ländern eingerichteten E-Justice-Gremien und –Verantwortlichen eng zusammen zu arbeiten.
>
> 2. Soweit Gegenstände des IT-Planungsrats den Einsatz der Informationstechnik in der Justiz betreffen, sind die aus den verfassungs- und einfachrechtlich garantierten Positionen der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten zu beachten. Die richterliche Unabhängigkeit ist zu wahren
>
> 3. Im Rahmen der Beteiligung der Justizministerkonferenz durch den IT-Planungsrat wird die Einhaltung der in Ziffer 2 genannten Grundsätze geprüft. Die Beteiligung erfolgt vor dem Abschluss der in Bund und Ländern notwendigen Abstimmungen des vorgesehenen Beschlusses."

3. Grenzen der Flexibilität bei der Finanzierung von ZaPuK als Produkt des IT-PLR

Die Finanzierung von Projekten und Produkten der FITKO erfolgt gemäß § 9 Abs. 4 IT-StV regelmäßig über den sogenannten modifizierten Königsteiner Schlüssel, nach dem die Bundesländer anteilig, je nach Steueraufkommen und Bevölkerungszahl, sowie der Bund zu einem festen Anteil von 25% die erforderlichen Mittel zur Verfügung stellen. Die insoweit vorgesehene Verteilung der Finanzierungsanteile ist grundsätzlich auch maßgeblich, soweit ZaPuK als

ein Produkt des IT-Planungsrats von der FITKO bereitgestellt und betrieben werden soll. Es stellt sich jedoch – insbesondere auch vor dem Hintergrund der zum Finanzierungsmodell des Deutschland-Stacks gefassten Beschlüsse des IT-Planungsrats, B-2026/18-IT vom 17. Juni 2026 – die Frage, ob und inwieweit diesbezüglich Flexibilität besteht und wo die Grenzen einer abweichenden Finanzierungsregelung gegebenenfalls liegen.

Solche Grenzen können sich bei Nutzung der vorhandenen Strukturen und Regelungen des IT-Staatsvertrags auf zwei Ebenen ergeben:

- Einfachgesetzlich ist zunächst die nähere Ausgestaltung der Finanzierung von Produkten des IT-Planungsrats in **§ 9 IT-StV** zu beachten. Dieser enthält in seinem Absatz 4 Satz 1 Halbsatz 2 eine Öffnungsklausel, nach der im Wirtschaftsplan auch Regelungen getroffen werden können, die vom modifizierten Königsteiner Schlüssel abweichen. Der insoweit maßgebliche Wirtschaftsplan wird gemäß § 9 Abs. 3 IT-StV durch den IT-Planungsrat beschlossen. Zustimmen müssen danach allerdings zusätzlich die Finanzministerkonferenz und das Bundesministerium des Innern; letzteres zudem im Einvernehmen mit dem Bundesfinanzministerium.

  Fraglich ist allerdings, ob diese Abweichungsmöglichkeit vollumfänglich für die Entwicklung, die Bereitstellung und den Betrieb von ZaPuK Anwendung finden kann. Denn § 9 Abs. 4 Satz 4 IT-StV enthält neben Satz 1 eine weitere Regelung zur Finanzierung nach dem modifizierten Königsteiner Schlüssel in Satz 4, allerdings ohne eine entsprechende Abweichungsmöglichkeit im Rahmen des Wirtschaftsplans vorzusehen. Nach Wortlaut und Systematik der Norm spricht daher viel dafür, dass diese Regelung sich auf all jene Aufgaben des IT-Planungsrats bzw. der FITKO bezieht, die auf § 1 Abs. 1 Satz 1 Nr. 4 und 5 IT-StV beruhen und daher in § 9 Abs. 2 IT-StV in Bezug genommen sind.

  Ein Blick auf die historische Entwicklung der Regelungen zeigt demgegenüber ein unklares Bild. Einerseits ließe sich aus der mit dem Zweiten IT-Änderungsstaatsvertrag vorgenommenen Anpassung des § 9 Abs. 4 Satz 1 Halbsatz 2 IT-StV auf eine

Erweiterung des Anwendungsbereichs der Öffnungsklausel schließen.[418] Andererseits deutet die Genese des Absatzes 4 aber zugleich darauf hin, dass für den Bereich der Produktsteuerung Satz 4 (und nicht Satz 1) Anwendung finden sollte: § 9 Abs. 2 IT-StV enthielt in der Fassung seit dem Ersten IT-Änderungsstaatsvertrag zunächst die Regelung eines einmalig von Bund und Ländern bereitgestellten Digitalisierungsbudgets, welches gemäß § 9 Abs. 4 Satz 4 IT-StV a.F. zu 35% durch den Bund und zu 65% anteilig von den Ländern getragen werden sollte. Dieses wurde mit dem Zweiten IT-Änderungsstaatsvertrag durch ein dauerhaftes, im Rahmen des Stammbudgets eingerichtetes Projektbudget abgelöst, welches „Projekte und Produkte für die Digitalisierung von Verwaltungsleistungen, die auf allen föderalen Ebenen zum Einsatz kommen" unterstützen und vorantreiben sollte und ausdrücklich auf § 1 Abs. 1 Satz 1 Nr. 4 und 5 IT-StV Bezug nimmt.[419]

Der letzteren Auslegung folgend wäre nur für den unter § 1 Abs. 1 Satz 1 Nr. 3 IT-StV zu subsumierenden Betrieb von ZaPuK die Möglichkeit eröffnet, untergesetzlich abweichende Regelungen für die Finanzierung zu treffen, also beispielsweise einen größeren Finanzierungsanteil des Bundes vorzusehen. Soweit dies auch für die Entwicklung und Bereitstellung der ZaPuK-Komponenten im Rahmen von § 1 Abs. 1 Satz 1 Nr. 4 und 5 IT-StV erfolgen soll, wäre demgegenüber – ähnlich den vormaligen Regelungen zum Digitalisierungsbudget 2020 bis 2022 – die Aufnahme einer abweichenden Regelung auf staatsvertraglicher Ebene zu empfehlen.

- Darüber hinaus sind **verfassungsrechtliche Grenzen** zu beachten. Wie bereits unter D.I.2.2.3.c) und D.I.2.3. ausgeführt worden ist, erlaubt Art. 91c Abs. 1, 2 GG als verfassungsrechtliche Grundlage des IT-StV durchaus verschiedene Ausgestaltungen zur Finanzierung der Planung, der Errichtung und des Betriebs der erforderlichen IT-Systeme. Art. 91c Abs. 1 GG kann insoweit als lex specialis zum u.a. in Art. 104a Abs. 1 GG

[418] Vgl. Gesetzentwurf der Bundesregierung, BR-Drucksache 237/24 vom 24.05.2024, S. 13. In § 9 Abs. 4 Satz 1 Halbsatz 2 IT-StV wurden im Rahmen der Öffnungsklausel die Worte „für einzelne Projekt oder Produkte" gestrichen.
[419] Vgl. Gesetzentwurf der Bundesregierung, BR-Drucksache 237/24 vom 24.05.2024, A.I. Zielsetzung und Notwendigkeit des Zweiten IT-Änderungsstaatsvertrages, S. 6.

verankerten Trennungs- und Konnexitätsprinzip verstanden werden.[420] Allerdings geht Art. 91c Abs. 1 GG dabei stets von einem „Zusammenwirken" von Bund und Ländern aus, er verleiht dem Bund gerade keine alleinige Gesetzeskompetenz und auch keine umfassende Finanzierungsbefugnis.[421] Die konkrete Ausgestaltung eines Betriebs- und Finanzierungsmodells auf Basis von Art. 91c Abs. 1 GG muss daher bei funktionaler Gesamtbetrachtung den kooperativen Charakter des Zusammenwirkens wahren. Eine Abweichung hiervon wäre – ohne eine entsprechende Verfassungsänderung – auch mit Zustimmung aller Beteiligten nicht zulässig.[422]

Vor diesem Hintergrund sprechen aus unserer Sicht überwiegende Gründe dafür, dass die verfassungsrechtliche Grundlage jedenfalls eine völlig einseitige Verortung von Verantwortlichkeiten und Lasten auf Seiten des Bundes nicht tragen würde. Diese Sicht entspricht auch der bisherigen Staatspraxis im Rahmen des Art. 91c GG. So wurden beispielsweise für das Digitalisierungsbudget der FITKO für 2020-2022 sowie für die Umsetzung von NOOTS ab 2027 jeweils höhere Finanzierungsanteile des Bundes festgelegt. Mit 35% Bundesanteil gemäß § 9 Abs. 4 Satz 4 IT-StV a.F. beziehungsweise mit einem zusätzlichen Beitrag des Bundes in Höhe von 46,6% der Gesamtkosten[423] bewegen sich diese jedoch in einem Rahmen, der nicht die Wortlautgrenzen des „Zusammenwirkens" sprengt. Bei einem Bundesanteil von 90 bis 100% wäre eine Verortung in Art. 91c Abs. 1 GG hingegen aus unserer Sicht mit erheblichen Risiken behaftet.

Je nach konkreter Ausgestaltung der Finanzierungsanteile dürfte sich im Anschluss auch die Frage nach einer dem Finanzierungsanteil angemessenen Einflussnahme des Bundes auf Entscheidungen im Zusammenhang mit ZaPuK stellen. Da das Produktmanagementmodell einschließlich seiner Gremienstruktur untergesetzlich, auf Basis eines IT-Planungsrats-Beschlusses

[420] Siehe unter D.I.2.2.3.c) und D.I.1.3.1.
[421] Vgl. M. Martini, in: von Münch/Kunig, Grundgesetz Kommentar, Band 2, Art. 70-146, Kämmerer/Kotzur (Hrsg.), 8. Auflage, Art. 91c, Rn. 20; vgl. auch: Wissenschaftlicher Dienst des Deutschen Bundestages, Gesetzgebungskompetenzen im Bereich des „Digitalpakts Schule", Ausarbeitung WD 3 – 3000 – 101/18, S. 3 und 4.
[422] Vgl. bereits grundlegend unter D.I.1.3.3. mit weiteren Nachweisen, sowie BVerfG, Beschluss vom 07.12.2021 – 2 BvL 2/15, Rn. 54.
[423] Siehe § 8 Abs. 1 NOOTS-Staatsvertrag; im Zusammenspiel mit dem in § 9 IT-StV vorgesehenen Bundesanteil von 25% ergibt sich daraus ein Gesamtanteil des Bundes von rund 60%.

konkretisiert worden ist,[424] können auch entsprechende Anpassungen der diesbezüglichen Governance auf dieser Ebene getroffen werden. Allerdings sind auch insoweit die soeben aufgezeigten Grenzen zu beachten. Auch innerhalb der Strukturen der FITKO steht der zugrundeliegende Art. 91c Abs.1 GG in seinem Anwendungsbereich einer vollständigen Aufgabe des „Zusammenwirkens" entgegen. Sollen zudem Governance-Regelungen getroffen werden, die über die FITKO-internen Strukturen des Produktmanagements hinausreichen – zum Beispiel weil sie die Zusammenarbeit mit weiteren verantwortlichen Stellen betreffen -, so würde allein eine Anpassung des internen Produktmanagementmodells dafür keine hinreichende Grundlage bieten (siehe auch sogleich unter 4.).

4. Governance des ZaPuK-Kommunikationsverbunds

Wird ZaPuK auf Basis des IT-Staatsvertrags in das Produktmanagement der FITKO integriert, so sind damit noch keine Regelungen getroffen, welche die Governance spezifisch für den ZaPuK-Kommunikationsverbund ausgestalten. Ein diesbezüglicher Regelungsbedarf entsteht insbesondere auch daraus, dass der Betrieb der zentralen Backends auf mehrere verantwortliche Stellen – beim Bund und bei der FITKO – verteilt werden soll (vgl. Architekturkonzept, Abschnitt 4.2.3). Für Themen wie die strategische Weiterentwicklung von ZaPuK (auch im Zusammenspiel mit den weiteren Basiskomponenten des D-Stacks), die gemeinsame Festlegung und die Sicherstellung der Einhaltung der Anschlussbedingungen, Eskalationsmechanismen oder das Anbindungsmanagement[425] sind vor diesem Hintergrund übergreifende Governance-Strukturen und damit auch entsprechende zusätzliche Regelungen oder Vereinbarungen – jenseits des bestehenden IT-Staatsvertrags – erforderlich.[426]

Das Architekturkonzept verweist in diesem Zusammenhang richtigerweise darauf, dass die für ZaPuK erforderliche Governance-Struktur in sachgerechter Weise nur in Abstimmung mit den zurzeit in Ausarbeitung befindlichen Strukturen des Deutschland-Stacks erfolgen kann. Doppelte Governance-Strukturen für die verschiedenen Bausteine des D-Stacks sollen

[424] Siehe Gesamtdokumentation zu Beschluss B-2024/51-IT, Produktmanagement-Modell für die Produkte des IT-Planungsrats, Version 1.0, Stand: 30.09.2024, Abschnitt 4.
[425] Vgl. für eine ausführliche Auflistung: Architekturkonzept, Abschnitt 4.3.
[426] Ein Vorbild könnten insoweit die im Rahmen des NOOTS-Staatsvertrags getroffenen Governance-Regelungen für das Zusammenspiel von FITKO und Bundesverwaltungsamt sein.

demgegenüber vermieden werden. Die spezifischen Bedarfe von ZaPuK sind dementsprechend bei der Ausarbeitung und Kodifizierung der Governance des D-Stacks zu berücksichtigen, wobei abzuwarten bleibt, in welcher Form und in welchem Rahmen die insoweit erforderlichen Regelungen getroffen werden.[427]

5. Weiterhin weitere gesetzliche Regelungen erforderlich

Unabhängig von der Frage nach einer über die aktuelle Fassung des IT-Staatsvertrags hinausgehenden staatsvertraglichen Lösung besteht im Hinblick auf ZaPuK ergänzender gesetzlicher Regelungsbedarf. Dies betrifft insbesondere das OZG, dessen Anpassung auf Grundlage von Art. 91c Abs. 5 GG erfolgen kann. Hierzu zählen etwa die rechtliche Entkopplung des Postfachbegriffs von den OZG-Nutzerkonten (siehe D.II.2.2.2.; D.II.2.2.2.b)aa); D.II.2.2.2.b)bb)) oder die Schaffung einer Rechtsgrundlage für die Datenverarbeitung (siehe D.III.1.2.7.).

Darüber hinaus sind unter anderem Änderungen der jeweils einschlägigen verwaltungsverfahrensrechtlichen Vorschriften zur Bekanntgabe von Verwaltungsakten erforderlich (siehe D.II.2.2.2.b)cc); D.II.2.2.2.b)gg)). Für den Bereich der Steuerverwaltung kommt insoweit beispielsweise eine Anpassung der entsprechenden Regelungen der Abgabenordnung auf Grundlage von Art. 108 Abs. 5 GG in Betracht.

Soll zudem eine verbindliche Anbindung der Länder (einschließlich der Kommunen) an ZaPuK gesetzlich vorgegeben werden, kann dies aus unserer Sicht ebenfalls über das OZG auf Basis von Art. 91c Abs. 5 GG erfolgen (siehe D.I.2.2.2.c)). Denkbar wäre aber insofern auch eine Verankerung in einer staatsvertraglichen Regelung.

IV. Mehrwert eines eigenständigen Staatsvertrags bzw. ergänzender staatsvertraglicher Regelungen

In den vorstehenden Abschnitten ist deutlich geworden, dass eine Umsetzung von ZaPuK auf Grundlage des bestehenden IT-Staatsvertrags und in den Produktmanagement-Strukturen von IT-Planungsrat und FITKO rechtlich nicht ausgeschlossen ist, dass aber aus der Nutzung dieses

[427] Vorstellbar wären z.B. ein eigener „D-Stack-Staatsvertrag“ auf Grundlage von Art. 91c Abs. 1, 2 GG oder eine entsprechende Erweiterung des IT-Staatsvertrags.

Modells bestimmte rechtliche Restriktionen folgen, die bei der Umsetzung zu berücksichtigen sind.

Wir halten es vor diesem Hintergrund für vorzugswürdig, die bestehenden staatsvertraglichen Regelungen um weitere zu ergänzen. Konkret ergibt sich deren rechtlicher Mehrwert gegenüber der bloßen Nutzung der vorhandenen Regelungen und Strukturen aus den folgenden Aspekten:

- Eine funktionierende übergreifende Governance für den ZaPuK-Kommunikationsverbund setzt die Festlegung zusätzlicher Mechanismen und Regelungen, u.a. für die strategisch-organisatorische Abstimmung zwischen den rechtlich an verschiedenen Stellen verorteten Backend-Betreibern voraus (siehe oben unter III.4). Die insoweit erforderlichen Regelungen reichen über den Bereich innerer Organisation des IT-Planungsrats sowie über die bestehenden Regelungen des IT-Staatsvertrags hinaus. Vor diesem Hintergrund bietet es sich an, in Gestalt zusätzlicher staatsvertraglicher Regelungen auf Basis von Art. 91c Abs. 1, 2 GG für die nötigen Strukturen und Mechanismen zu sorgen. Aus Gründen der Rechtsklarheit und Transparenz ist insofern auch zu empfehlen, dass die Regelungen auf staatsvertraglicher, d.h. im Ergebnis gesetzlicher Ebene, und nicht lediglich durch Verwaltungsvereinbarung geregelt werden. Dafür sprechen nach der verfassungsrechtlichen Wesenslehre insbesondere auch die Auswirkungen, die solche übergreifenden Vereinbarungen gegebenenfalls auf das verfassungsrechtlich verankerte Gefüge der Verwaltungskompetenzen zwischen Bund und Ländern haben.

- Zugleich können die soeben angesprochenen Governance-Regelungen in staatsvertraglicher Form auch zum Anlass genommen werden, zwischen Bund und Ländern übergreifende Regelungen für den gesamten Deutschland-Stack zu vereinbaren. ZaPuK könnte so effizient in die Governance des Deutschland-Stacks integriert und für das Gesamtgefüge eine Dopplung oder Inkonsistenz von Governance-Regelungen und Gremienstrukturen vermieden werden.

- Ein Mehrwert zusätzlicher staatsvertraglicher Regelungen für ZaPuK könnte zudem darin bestehen, die genaue Ausgestaltung einer verbindlichen Anbindung der Länder und

insbesondere der Kommunen in konsensualer Weise zu regeln. Nicht ausgeschlossen ist aber ebenso eine Herstellung der Verbindlichkeit auf Basis von Art. 91c Abs. 5 GG (s.o. unter III.5). Ebenso könnte die perspektivisch angestrebte Ablösung bestehender Postfach- und Kommunikationslösungen bzw. die diesbezüglichen Übergangsregelungen Gegenstand einer staatsvertraglichen Regelung sein.

- Schließlich bietet eine Regelung auf staatsvertraglicher Ebene Vorteile, sofern für ZaPuK eine spezifische Finanzierungsregelung – zum Beispiel mit einem erhöhten Finanzierungsanteil des Bundes – getroffen werden soll. Wie unter III.3 gezeigt worden ist, besteht Rechtsunsicherheit hinsichtlich der Frage, inwieweit eine abweichende Regelung im Wirtschaftsplan des IT-Planungsrats, d.h. auf untergesetzlicher Ebene, im Hinblick auf die Entwicklung, Bereitstellung und Produktsteuerung getroffen werden kann. Eine Anpassung der Finanzierungsquoten auf staatsvertraglicher Ebene – wie dies in der Vergangenheit mit Blick auf das einmalige Digitalisierungsbudget bereits einmal erfolgt ist – wäre daher vorzugswürdig. Allerdings kann auch eine staatsvertragliche Regelung nicht die verfassungsrechtlichen Bedenken beseitigen, die gegenüber einer Regelung bestehen, die dem Bund hinsichtlich eines Produkts des IT-Planungsrates auf Basis von Art. 91c Abs. 1 GG eine hundertprozentige Finanzierungsverantwortlichkeit zuschreibt (siehe oben unter III.3), diesen wäre auf verfassungsrechtlicher Ebene zu begegnen.

***

Anhang

Verzeichnis gesetzlicher Regelungen

Abkürzung	Titel/Kurztitel	Fassung und Quelle
AEUV	Vertrag über die Arbeitsweise der Europäischen Union	in der Fassung der Bekanntmachung vom 9. Mai 2008 (ABl. 2016 C 202 S. 47, ber. ABl. C 400 S. 1), zuletzt geändert durch Art. 2 Änd-Beschl. 2012/419/EU vom 11.7.2012 (ABl. L 204 S. 131).
AO	Abgabenordnung	in der Fassung der Bekanntmachung vom 23. Januar 2025 (BGBl. 2025 I Nr. 24), die zuletzt durch Artikel 15 Absatz 6 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert worden ist.
ArbGG	Arbeitsgerichtsgesetz	in der Fassung der Bekanntmachung vom 2. Juli 1979 (BGBl. I S. 853, 1036), das zuletzt durch Artikel 7 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geändert worden ist.
ATDG	Antiterrordateigesetz	vom 22. Dezember 2006 (BGBl. I S. 3409), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 30. März 2021 (BGBl. I S. 402) geändert worden ist.

AufenthG	Aufenthaltsgesetz	in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 13 des Gesetzes vom 22. Juli 2026 (BGBl. 2026 I Nr. 222) geändert worden ist.
BArchG	Bundesarchivgesetz	in der Fassung der Bekanntmachung vom 6. September 2021 (BGBl. I S. 4122), das durch Artikel 26 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2759) geändert worden ist.
BDSG	Bundesdatenschutzgesetz	vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 3 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert worden ist.
BEEG	Bundeselterngeld- und Elternzeitgesetz	in der Fassung der Bekanntmachung vom 27. Januar 2015 (BGBl. I S. 33), das zuletzt durch Artikel 19 Absatz 2 des Gesetzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 370) geändert worden ist.
BEHG	Brennstoffemissionshandelsgesetz	vom 12. Dezember 2019 (BGBl. I S. 2728; 2022 I S. 2098), das zuletzt durch Artikel 2 des Gesetzes vom 27. Februar 2025 (BGBl. 2025 I Nr. 70) geändert worden ist.

BGB	Bürgerliches Gesetzbuch	in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 6 des Gesetzes vom 23. Juli 2026 (BGBl. 2026 I Nr. 226) geändert worden ist.
BRAO	Bundesrechtsanwaltsordnung	in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 4 des Gesetzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 349) geändert worden ist.
BSIG	BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301, S. 2), das zuletzt durch Artikel 8 Absatz 1 des Gesetzes vom 23. Juli 2026 (BGBl. 2026 I Nr. 226) geändert worden ist.
BSI-KritisV	BSI-Kritisverordnung	Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 3 Absatz 1 des Gesetzes vom 15. Mai 2026 (BGBl. 2026 I Nr. 148) geändert worden ist.

BSI TR-02102-2	BSI–Technische Richtlinie Kryptographische Verfahren	BSI–Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS) Version 2026-01.
DDG	Digitale-Dienste-Gesetz	vom 6. Mai 2024 (BGBl. 2024 I Nr. 149), das zuletzt durch Artikel 1 des Gesetzes vom 12. Mai 2026 (BGBl. 2026 I Nr. 138) geändert worden ist.
De-Mail-G	De-Mail-Gesetz	vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 4 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert worden ist.
DIdG-E	Digitale Identitätengesetz (Entwurfsfassung)	Gesetzentwurf der Bundesregierung zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvor-schriften vom 29.07.2026 (Drs. 21/7408).
Richtlinie (EU) 2025/25	Digitalisierungsrichtlinie	Richtlinie (EU) 2025/25 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Richtlinien 2009/102/EG und (EU) 2017/1132 zur Ausweitung und Optimierung des Einsatzes digitaler Werkzeuge und Verfahren im Gesellschaftsrecht (ABl. L, 2025/25, 10.1.2025).

DSGVO	Datenschutz-Grundverordnung	Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Da-tenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 04.05.2016, S. 1, ber. ABl. L 314 vom 22.11.2016, S. 72, ABl. L 127 vom 23.5.2018, S. 2, ABl. L 074 vom 4.3.2021, S. 35).
EDSA	Entwurf der EDSA-Leitlinien 02/2026	Guidelines 02/2026 on Anonymisation Version 1.0 Adopted on 07 July 2026 by the European Data Protection Board.
EGAO	Einführungsgesetz zur Abgabenordnung	vom 14. Dezember 1976 (BGBl. I S. 3341; 1977 I S. 667), das zuletzt durch Artikel 4 des Gesetzes vom 29. Juni 2026 (BGBl. 2026 I Nr. 197) geändert worden ist.
EGovG	E-Government-Gesetz des Bundes	vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 11 des Gesetzes vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301) geändert worden ist.
EGovG NRW	E-Government-Gesetz Nordrhein-Westfalen	E-Government-Gesetz Nordrhein-Westfalen vom 16. Juli 2016 (GV. NRW. S. 551), das zuletzt durch Artikel 5 Absatz 1 des Gesetzes

		vom 10. Dezember 2024 (GV. NRW. S. 1184) geändert worden ist.
eIDAS-VO	eIDAS-Verordnung	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 S. 73, ber. ABl. 2015 L 23 S. 19 und ABl. 2016 L 155 S. 44), zuletzt geändert durch Art. 1 VO (EU) 2024/1183 vom 11.4.2024 (ABl. L, 2024/1183, 30.4.2024, ABl. L, 2025/90317, 9.4.2025).
eIDKG	eID-Karte-Gesetz	vom 21. Juni 2019 (BGBl. I S. 846), das zuletzt durch Artikel 6 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 322) geändert worden ist.
EMRK	Europäische Menschenrechtskonvention	Konvention zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung vom 22. Ok-tober 2010 (BGBl. 2010 II S. 1198), die zuletzt durch EMRK-Protokoll Nr. 15 vom 24.6.2013 (BGBl. 2014 II S. 1034, 1035) geändert worden ist.
ePrivacy-Richtlinie	ePrivacy-Richtlinie	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener

		Daten und den Schutz der Privatsphäre in der elektroni-schen Kommunikation (Daten-schutzrichtlinie für elektronische Kommuni-kation) (ABl. L 201 S. 37), zuletzt geändert durch Art. 2 RL 2009/136/EG vom 25.11.2009 (ABl. L 337 S. 11, ber. 2013 ABl. L 241 S. 9, ber. 2017 ABl. L 162 S. 56).
ERVV	Elektronischer-Rechtsver-kehr-Verordnung	Verordnung über die technischen Rahmen-bedingungen des elektronischen Rechtsver-kehrs und über das besondere elektronische Behördenpostfach vom 24. November 2017 (BGBl. I S. 3803), die zuletzt durch Artikel 2 des Gesetzes vom 22. Juni 2026 (BGBl. 2026 I Nr. 192) geändert worden ist.
	Europäischer Kodex für die elektronische Kommunika-tion	Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezem-ber 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 S. 36, ber. ABl. 2019 L 334 S. 164), zuletzt ge-ändert durch Art. 43 RL (EU) 2022/2555 vom 14.12.2022 (ABl. L 333 S. 80).
FGO	Finanzgerichtsordnung	in der Fassung der Bekanntmachung vom 28. März 2001 (BGBl. I S. 442, 2262; 2002 I S. 679), die zuletzt durch Artikel 12 Absatz 2 des Geset-zes vom 29. Juni 2026 (BGBl. 2026 I Nr. 197) geändert worden ist.

FVG	Finanzverwaltungsgesetz	in der Fassung der Bekanntmachung vom 4. April 2006 (BGBl. I S. 846, 1202), das zuletzt durch Artikel 4 des Gesetzes vom 26. Mai 2026 (BGBl. 2026 I Nr. 156) geändert worden ist.
	Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern	Gesetz für den Bürokratierückbau im Bereich des Bundesministeriums des Innern vom 03.07.2026 (BGBl. 2026 I Nr. 199)
	Gesetz zur Einführung der elektronischen Akte in der Justiz	Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 (BGBl. I S. 2208)
	Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten	Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. 2013 I Nr. 62 S. 3786).
	Gesetz zur Neuregelung des bundesstaatlichen Finanzausgleichssystems	Gesetz zur Neuregelung des bundesstaatlichen Finanzausgleichssystems ab dem Jahr 2020 und zur Änderung haushaltsrechtlicher Vorschriften vom 14.08.2017 (BGBl. 2017 I S. 3122).
GG	Grundgesetz	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt

		Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 22. März 2025 (BGBl. 2025 I Nr. 94) geändert worden ist.
GrCh	EU-Grundrechtecharta	Charta der Grundrechte der Europäischen Union, (ABl. C 202 vom 07.06.2016, S. 389).
HInschG	Hinweisgeberschutzgesetz	Hinweisgeberschutzgesetz vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), das zuletzt durch Artikel 2 des Gesetzes vom 22. Juli 2026 (BGBl. 2026 I Nr. 223) geändert worden ist.
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder	Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG) vom 10. Au-gust 2009 (BGBl. 2009 I S. 2702, 2706), das zuletzt durch Artikel 3 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert worden ist.
ITSiV-PV	IT-Sicherheitsverordnung Portalverbund	Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten vom 6. Januar 2022 (BGBl. I S. 18).
IT-StV	IT-Staatsvertrag	Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der

		Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern - Vertrag zur Ausführung von Artikel 91c GG vom 30. Oktober 2009 bis 30. November 2009 (BGBl. 2010 I S. 662), der durch Staatsvertrag vom 15. bis 21. März 2019 (BGBl. 2019 I S. 1126) und zuletzt durch Staatsvertrag vom 27. November bis 31. Dezember 2023 (BGBl. 2024 I Nr. 326) geändert worden ist.
JI-Richtlinie	JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zu-ständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 S. 89, ber. 2018 L 127 S. 9 und 2021 L 74 S. 36).
KONSENS-G	KONSENS-Gesetz	Gesetz über die Koordinierung der Entwicklung und des Einsatzes neuer Software der Steuer-verwaltung vom 14. August 2017 (BGBl. I S. 3122, 3129).

KRITIS-Dach-gesetz	KRITIS-Dachgesetz	KRITIS-Dachgesetz vom 11. März 2026 (BGBl. 2026 I Nr. 66), das durch Artikel 8 des Gesetzes vom 21. Juli 2026 (BGBl. 2026 I Nr. 221) geändert worden ist.
NIS-2-Richtlinie	NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022 S. 80).
NOOTS-StV	NOOTS-Staatsvertrag	Vertrag über die Errichtung, den Betrieb und die Weiterentwicklung des Nationalen Once-Only-Technical-Systems (NOOTS) – Vertrag zur Ausführung von Artikel 91c Absatz 1, Absatz 2 GG – NOOTS-Staatsvertrag (BGBl. 2025 I Nr. 325, S. 3; 2026 I Nr. 35).
OZG	Onlinezugangsgesetz	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 21 des Gesetzes vom 22. Juli 2026 (BGBl. 2026 I Nr. 224) geändert worden ist.

PAO	Patentanwaltsordnung	Patentanwaltsordnung vom 7. September 1966 (BGBl. I S. 557), die zuletzt durch Artikel 12 Ab-satz 3 des Gesetzes vom 29. Juni 2026 (BGBl. 2026 I Nr. 197) geändert worden ist.
PAuswG	Personalausweisgesetz	Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 3 des Gesetzes vom 16. Juli 2026 (BGBl. 2026 I Nr. 213) geändert worden ist.
Richtlinie (EU) 2015/1535	Richtlinie (EU) 2015/1535	Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der In-formationsgesellschaft (ABl. L 241 vom 17.9.2015 S.1).
SGB I	Sozialgesetzbuch Erstes Buch	Das Erste Buch Sozialgesetzbuch – Allgemei-ner Teil – (Artikel I des Gesetzes vom 11. De-zem-ber 1975, BGBl. I S. 3015), das zuletzt durch Artikel 3 des Gesetzes vom 22. Juli 2026 (BGBl. 2026 I Nr. 223) geändert worden ist.
SGB V	Sozialgesetzbuch Fünftes Buch	Das Fünfte Buch Sozialgesetzbuch – Gesetz-liche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S.

		2477, 2482), das zuletzt durch Artikel 1 des Gesetzes vom 24. Juli 2026 (BGBl. 2026 I Nr. 228) geändert worden ist.
SGB X	Sozialgesetzbuch Zehntes Buch	Das Zehnte Buch Sozialgesetzbuch – Sozial-verwaltungsverfahren und Sozialdaten-schutz – in der Fassung der Bekanntma-chung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Arti-kel 6 des Gesetzes vom 21. Juli 2026 (BGBl. 2026 I Nr. 221) ge-ändert worden ist.
SGG	Sozialgerichtsgesetz	in der Fassung der Bekanntmachung vom 23. September 1975 (BGBl. I S. 2535), das zuletzt durch Artikel 8 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geän-dert wor-den ist.
StBerG	Steuerberatungsgesetz	in der Fassung der Bekanntmachung vom 4. November 1975 (BGBl. I S. 2735), das zuletzt durch Artikel 1 des Gesetzes vom 29. Juni 2026 (BGBl. 2026 I Nr. 197) geändert worden ist.
StPO	Strafprozessordnung	in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 15 Absatz 16 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert worden ist.

TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Ar-tikel 3 des Gesetzes vom 10. März 2026 (BGBl. 2026 I Nr. 64) geändert worden ist.
TKG	Telekommunikationsgesetz	vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 2 des Gesetzes vom 12. Mai 2026 (BGBl. 2026 I Nr. 138) geändert worden ist.
TKÜV	Telekommunikations-Überwachungsverordnung	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 11 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist.
TMG	Telemediengesetz	vom 26.02.2007 (BGBl. I S. 179), das aufgrund Gesetzes vom 06.05.2024 (BGBl. I S. 149) m.W.v. 14.05.2024 außer Kraft getreten ist.
UBRegG	Unternehmensbasisdatenregistergesetz	vom 9. Juli 2021 (BGBl. I S. 2506), das zuletzt durch Artikel 11 des Gesetzes vom 22.

		Dezember 2025 (BGBl. 2025 I Nr. 354) geändert worden ist.
Verordnung (EU) 2021/1232	Verordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern	Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger inter-personeller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet (Abl. L 274 vom 30.7.2021 S. 41), zuletzt geändert durch Art. 1 VO (EU) 2024/1307 vom 29.4.2024 (ABl. L, 2024/1307, 14.5.2024). Im Juli 2026 bis 3. April 2028 verlängert.
CSA-Verordnung		Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vom 11.5.2022 (COM(2022)209).
Vorschlag COM(2025)838		Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung europäischer

		Unternehmensbrieftaschen vom 19.11.2025 (COM(2025)838)
VWDG	Visa-Warndateigesetz	Gesetz zur Errichtung einer Visa-Warndatei vom 22. Dezember 2011 (BGBl. I S. 3037), das zuletzt durch Artikel 173 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.
VWGO	Verwaltungsgerichtsordnung	in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), die zuletzt durch Artikel 9 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geändert worden ist.
VwVfG	Verwaltungsverfahrensgesetz	Verwaltungsverfahrensgesetz des Bundes in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 11 des Gesetzes vom 22. Juli 2026 (BGBl. 2026 I Nr. 224) geändert worden ist.
VWZG	Verwaltungszustellungsgesetz	Verwaltungszustellungsgesetz des Bundes vom 12. August 2005 (BGBl. I S. 2354), das zuletzt durch Artikel 15 Absatz 3 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert wor-den ist.
ZPO	Zivilprozessordnung	in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel

		3 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geändert worden ist.

Abbildungsverzeichnis

Abbildung 1: Vollzugszuständigkeiten und Regelungsbefugnisse – Überblick 39

Tabellenverzeichnis

Tabelle 1: Folgerungen für ZaPuK 24

Tabelle 2: Anregungen und Empfehlungen für Rechtsänderungen 28