PLANIT // LEGAL

Rechtsgutachten zur datenschutzrechtlichen Neukonzeption der Online-Sicherheitsprüfung (OSiP)

Fassung vom 21. Januar 2026

(Öffentliche Bereitstellung)

Herausgeberin und Lizenzgeberin:

FITKO (Föderale IT-Kooperation)

Anstalt des öffentlichen Rechts

Erstellt durch:

Dr. Bernhard Freund, M.Comp.Sc., LL.M. (Wellington), Nils Eckert

PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH

Inhaltsverzeichnis

A. Einleitung und Prüfauftrag

I. Auftraggeberin und Auftrag

Die Föderale IT-Kooperation (FITKO), eine rechtsfähige Anstalt des öffentlichen Rechts in gemeinsamer Trägerschaft von Bund und Ländern mit Sitz in Frankfurt am Main, hat die PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH mit der Erstellung eines Rechtsgutachtens zur datenschutzrechtlichen Neukonzeption des Produkts „Online-Sicherheitsprüfung" (OSiP) beauftragt.

Die FITKO unterstützt den IT-Planungsrat bei der Umsetzung seiner Beschlüsse zur Digitalisierung der Verwaltung in Deutschland. Hierzu zählen insbesondere die Planung und Koordination gemeinsamer IT-Vorhaben von Bund und Ländern, die Vernetzung der beteiligten Akteurinnen und Akteure sowie die fachliche Begleitung strategischer Digitalisierungsprojekte.

II. Ziel und Zweck des Gutachtens

Ziel des Gutachtens ist die rechtliche Bewertung der geplanten Neukonzeption und Zielarchitektur von OSiP, eines durch den IT-Planungsrat gesteuerten und in mehreren Bundesländern bereits eingesetzten digitalen Verfahrens zur Durchführung gesetzlich vorgeschriebener Zuverlässigkeits- und Sicherheitsüberprüfungen (ZSÜ).

Im Mittelpunkt steht die Klärung der rechtlichen Voraussetzungen, Optionen und Grenzen für eine geeignete Zielarchitektur. Die Fragestellung wird in einem Fragenkatalog konkretisiert und systematisch beantwortet.

Gegenstand der Prüfung ist insbesondere, ob und unter welchen Bedingungen der derzeit dezentrale Betrieb in einen zentralen Betrieb unter Verantwortung der FITKO rechtlich tragfähig überführt werden kann. Die Zielarchitektur sieht eine zentrale OSiP-Transportinfrastruktur vor, in der der Datenaustausch zwischen den Fachverfahren der für ZSÜ zuständigen Behörden und den Fachverfahren der Erkenntnisstellen grundsätzlich Ende-zu-Ende verschlüsselt erfolgen soll. Nur die für Routing, Protokollierung und Betrieb technisch erforderlichen Metadaten (z.B. Absender, Empfänger, Zeitstempel) bleiben im Klartext. Neben der OSiP-Transportinfrastruktur wird unter Verantwortung der FITKO ein OSiP-Fachverfahren (Backend und Webserver/Frontend) für die für ZSÜ zuständigen Behörden bereitgestellt, die Länder können jedoch alternativ eigene Fachverfahren nutzen, die direkt mit der OSiP-Transport-Infrastruktur oder mit dem OSiP-Fachverfahren-Backend kommunizieren.

Das Gutachten untersucht hierfür die maßgeblichen rechtlichen Rahmenbedingungen und Voraussetzungen der Neugestaltung und berücksichtigt insbesondere

- die datenschutzrechtlichen Verantwortlichkeitskonstellationen nach der Datenschutz-Grundverordnung (Art. 4 Nr. 7, Art. 26, 28 DSGVO),
- die rechtlichen Anforderungen an einen zentralen oder föderalen Betrieb im Kontext gemeinsamer IT-Kooperationen von Bund und Ländern sowie
- die sich daraus ergebenden technischen und organisatorischen Mindestanforderungen nach DSGVO, IT-Sicherheitsgesetz, den BSI-Standards und ggf. sektorspezifischen Fachgesetzen.

Ziel ist, der FITKO eine Entscheidungs- und Bewertungsgrundlage für die Neukonzeption von OSiP bereitzustellen, datenschutzrechtliche und föderale Handlungsbedarfe zu identifizieren und konkrete Empfehlungen für eine rechtssichere, datenschutzkonforme und organisationsrechtlich tragfähige Systemgestaltung zu formulieren.

III. Gegenstand und Prüfungsfragen

Der Auftrag umfasst die Erstellung eines datenschutzrechtlich ausgerichteten Rechtsgutachtens zur rechtlichen Einordnung der Neukonzeption und des künftigen Betriebs von OSiP und zur Ableitung von Gestaltungsempfehlungen für System- und Betriebsarchitektur.

Im Zentrum stehen insbesondere folgende Prüfungsgegenstände:

- die Bestimmung der maßgeblichen europäischen und nationalen Rechtsgrundlagen für Betrieb und Datennutzung von OSiP,
- die Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten zwischen FITKO, Betreibern und Landesbehörden,
- die rechtlichen Voraussetzungen für einen zentralen bzw. länderübergreifenden Betrieb des Systems, einschließlich möglicher Alternativmodelle,
- die rechtlichen Anforderungen an technische und organisatorische Maßnahmen, IT-Sicherheitsstandards und Netzinfrastrukturen sowie
- die Verteilung von Verantwortlichkeiten und Haftung zwischen FITKO, Betreiber und Ländern im zukünftigen Betriebsmodell.

B. Sachverhalt – Online-Sicherheitsprüfung (OSiP)

Im folgenden Abschnitt wird der technische und organisatorische Aufbau des Produkts „Online-Sicherheitsprüfung“ (OSiP) dargestellt. Die Sachverhaltsdarstellung bildet die Grundlage für die anschließende rechtliche Analyse und Bewertung der geplanten Zielarchitektur sowie der damit verbundenen datenschutz- und organisationsrechtlichen Fragestellungen.

I. Allgemeine Beschreibung

Bei der Online-Sicherheitsprüfung (OSiP) handelt es sich um ein bundesweit einsetzbares IT-Verfahren zur digitalen Durchführung personenbezogener Zuverlässigkeits- und Sicherheitsüberprüfungen (ZSÜ). Ziel ist es, einen standardisierten und rechtssicheren Prüfprozess zu ermöglichen, der eine länderübergreifende Zusammenarbeit von Bürgerinnen und Bürgern, Unternehmen, Genehmigungsbehörden, Sicherheitsbehörden und Registerstellen gewährleistet.

Inhaltlich dient OSiP der in verschiedenen Fällen gesetzlich vorgeschriebenen Überprüfung von Personen zur Gewährleistung der Sicherheit und/oder Zuverlässigkeit. Hierzu zählt die Überprüfung einer Personen, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll (Sicherheitsüberprüfung, vgl. § 1 Abs. 1 SÜG); wobei eine sicherheitsempfindliche Tätigkeit insbesondere aus dem Zugang zu Verschlusssachen folgt (vgl. im Einzelnen § 1 Abs. 2 SÜG), aber auch aus dem Zugang zu besonders schutzwürdigen Anlagen oder Einrichtungen. Ferner zählen zu den ZSÜ die verschiedentlich spezialgesetzlich vorgeschriebenen Zuverlässigkeitsüberprüfungen, die zumeist einen gewerberechtlichen Einschlag haben (z.B. nach ProstSchG). Zu den Anwendungsfeldern und beteiligten Akteuren siehe im Einzelnen II. Damit bildet OSiP eine zentrale technische Infrastruktur zur Umsetzung gesetzlich vorgeschriebener Sicherheits- und Zuverlässigkeitsprüfungen nach Bundes- und Landesrecht in verschiedenen Fachrechtsbereichen.

OSiP wurde zum 01.04.2017 vom IT-Planungsrat als Anwendung übernommen,[1] nachdem es zuvor als Koordinierungsprojekt entwickelt worden war (ursprünglich von Nordrhein-Westfalen im Rahmen des EfA-Prinzips). Zum 01.02.2022 wurde es in das Produktportfolio des IT-Planungsrats bzw. der FITKO überführt.[2] Als Produkt des IT-Planungsrats wird OSiP von der FITKO gesteuert und in deren Auftrag (weiter-)entwickelt. Im Kompass der föderalen IT-Architektur

---

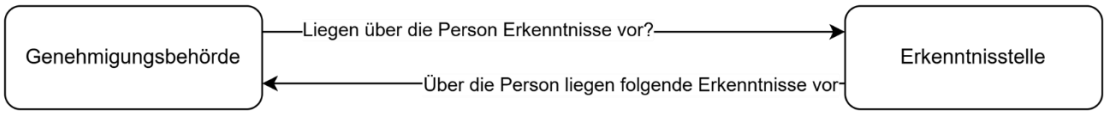
[1] IT-PLR, Beschluss 2017/12 (22. Sitzung) vom 22.03.2017.

[2] IT-PLR, Beschluss 2021/13 (34. Sitzung) vom 17.03.2021.

wird OSiP in der Schicht der Querschnittskomponenten/Basisdienste der Kategorie „Identität“ zugeordnet.[3]

Im Kern bildet OSiP die Kommunikations- und Verfahrenslogik zwischen den beteiligten Akteuren ab. Die digitale Plattform unterstützt die strukturierte und rechtssichere Übermittlung von Anträgen, Anfragen und Rückmeldungen zwischen Genehmigungsbehörden und Erkenntnisstellen. Nach Antragstellung sowie Erfassung und formaler Vorprüfung werden die zuständigen Erkenntnisstellen (insbesondere Landeskriminalämter, Landesämter für Verfassungsschutz und das Bundeszentralregister) über definierte Schnittstellen angefragt. Rückmeldungen der Erkenntnisstellen über vorliegende Erkenntnisse oder „keine Erkenntnis“ werden grundsätzlich über denselben technischen Kommunikationsweg an die anfragende Behörde zurückgeleitet. Eine Ausnahme bilden die Landesämter für Verfassungsschutz, die Erkenntnisse derzeit in Papierform übermitteln. Ein unmittelbarer Zugriff der anfragenden Behörde auf die IT-Systeme der Erkenntnisstellen besteht nicht. Nach Eingang der Rückmeldungen dieser Erkenntnisstellen trifft die fachlich zuständige Genehmigungsbehörde die Entscheidung über den Antrag.

Das folgende Schaubild veranschaulicht den Informationsfluss im Rahmen einer typischen Sicherheitsüberprüfung:



II. Anwendungsfelder und beteiligte Akteure

OSiP wird in sämtlichen Bereichen eingesetzt, in denen gesetzliche Vorschriften eine Zuverlässigkeits- oder Sicherheitsüberprüfung vorschreiben. Zu den zentralen Anwendungsfeldern zählen insbesondere:

- Luft- und Hafensicherheit (z.B. Flughafenausweise, sichere Lieferkette)
- Waffengesetz und Jagd (Erteilung von Waffenbesitzkarten, jagdrechtliche Überprüfungen)
- Einbürgerungs- und Aufenthaltsrecht (insbesondere über Prozesse des Bundesverwaltungsamts)

[3] Siehe https://docs.fitko.de/kompass/docs/it-landschaft/basisdienste/identitaet/osip/.

- Atomrechtliche Zuverlässigkeitsprüfung und KRITIS-nahe Bereiche (einschließlich Akkreditierung bei Großveranstaltungen)
- Militärischer Abschirmdienst (MAD)
- Gewerberecht und Strafvollzug (z.B. Bewachungsgewerbe, Prostituiertenschutzgesetz)
- Anlassbezogene Überprüfungen (z.B. Akkreditierungen)
- Justizvollzug und Überprüfung für Anstaltsfremde
- Sprengstoffgesetz

Die Zuständigkeiten für die Durchführung dieser Verfahren sind föderal differenziert und erstrecken sich über Bundes-, Landes- und Kommunalebene:

Ebene	Für ZSÜ zuständige Behörden (Beispiele)
Bund	Militärischer Abschirmdienst (MAD), Bundesverwaltungsamt (BVA)
Länder	Fachministerien (z.B. Ministerien für Umwelt, Inneres, Justiz)
Kommunen	Bezirksregierungen, Luftsicherheitsbehörden, Einbürgerungsbehörden, Ordnungs- und Jagdbehörden, Kreise, kreisfreie Städte, Justizvollzugsanstalten, Kreispolizeibehörden, Landeskriminalämter

Die folgende Übersicht zeigt beispielshaft in Nordrhein-Westfalen zuständige Behörden für ausgewählte Prüfbereiche:

Anwendungsbereich	Für ZSÜ zuständige Behörden (Beispiele)
Luftsicherheit	Bezirksregierungen Düsseldorf und Münster als Luftsicherheitsbehörden in NRW
Einbürgerung	Kreise, kreisfreie Städte und große kreisangehörige Städte als Einbürgerungsbehörden
Waffengesetz	Kreispolizeibehörden
Anlassbezogene Überprüfungen	Landeskriminalamt

Mehrere Bundesländer – darunter Nordrhein-Westfalen, Baden-Württemberg, Niedersachsen und Hamburg – setzen OSiP bereits produktiv ein oder planen den Roll-out (siehe V. zum Ist-Zustand). Das System wird zunehmend als gemeinsame Plattform für Sicherheitsüberprüfungen etabliert, die künftig durch die FITKO zentral betrieben und weiterentwickelt werden soll.

III. Erkenntnisstellen und Datenquellen

Die im Rahmen von OSiP angebundenen Erkenntnisstellen sind die zentralen Informationsgeber für die ZSÜ. Hierzu gehören insbesondere:

1. Polizeien und Nachrichtendienste

- Landeskriminalämter (LKA)
- Landesämter für Verfassungsschutz (LfV)
- Je nach Anwendungsbereich ggf. weitere Sicherheitsbehörden (z.B. das Bundeskriminalamt)

2. Zentrale Register

- Bundeszentralregister (BZR)
- Zentrales staatsanwaltschaftliches Verfahrensregister (ZStV)
- Gewerbezentralregister (GZR)
- Luftsicherheitsregister

Diese Stellen stellen sicherheitsrelevante Informationen über strafrechtliche Erkenntnisse, Verdachtsmomente, Aufenthaltsstatus oder gewerberechtliche Vorgänge bereit, die für die Entscheidung der Genehmigungsbehörden maßgeblich sind.

IV. Stakeholdergruppen und Austauschformate

Die organisatorische Struktur von OSiP umfasst mehrere Akteurs- und Steuerungsebenen, die für Betrieb, Weiterentwicklung und Governance verantwortlich sind:

1. ZSÜ-Ebene (operative Verfahrensebene)

- Antragstellende und Antragserfassungsstellen
- Genehmigungsbehörden (Bund, Länder, Bezirke)
- Erkenntnisstellen und Registerstellen

2. Gremien und Steuerungsinstanzen

- IT-Planungsrat (IT-PLR)
- Fachministerkonferenz
- Föderales IT-Architekturboard (FIT-AB) und Föderales IT-Architekturmanagement (FITKO-AM)
- Produktboard OSiP
- Lenkungsausschuss NEOSiP
- Fachgruppen und Community-Formate

Diese Gremien gewährleisten die föderale Steuerung und Qualitätssicherung des Systems und stimmen technische, organisatorische und rechtliche Anforderungen ab.

3. Technologische und Datenschutzebene

- Betreiberorganisation und Fachverfahrenshersteller
- OSiP-Entwicklungsteam
- Informationssicherheitsbeauftragte (ISB)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Landesdatenschutzbeauftragte und behördliche Datenschutzbeauftragte

Diese Akteure verantworten die Umsetzung der Anforderungen Informationssicherheit, Datenschutz und Systemintegrität.

V. Bestandssystem (Ist-Zustand)

Derzeit (seit 2017) wird OSiP im Auftrag der FITKO als Softwareprodukt entwickelt und den teilnehmenden Bundesländern zur Verfügung gestellt. Die Länder betreiben die Anwendung eigenständig über Landesbetreiber ihrer Wahl – beispielsweise Dataport, IT.NRW oder BITBW – jeweils in den Landesnetzen. Es besteht somit eine dezentrale Struktur, in der jedes Land eine eigene OSiP-Instanz mit eigenem Datenbestand betreibt.

1. Systemarchitektur (Ist-Zustand)

Im aktuellen Zustand besteht OSiP aus zwei zentralen Komponenten:

- dem OSiP-Kern, der als Transport- und Verarbeitungskomponente für den Datenaustausch zwischen Fachverfahren fungiert, und

- verschiedenen OSiP-Fachverfahren (OSiP-Clients), die optional zur Antragserfassung, Genehmigungsbearbeitung oder Erkenntniserfassung eingesetzt werden können.

Der OSiP-Kern stellt die technische Kommunikationsschnittstelle zwischen den beteiligten Systemen her. Über standardisierte SOAP-Schnittstellen (optional auch über CLI/XML-Dateiablage) können andere Fachverfahren von Drittanbietern (z.B. in Erkenntnisstellen) an den OSiP-Kern angebunden werden. Alle eingehenden Datenströme werden im OSiP-Kern validiert.

Die technische Architektur folgt in einem dreischichtigen Aufbau:

- Antragsebene (Front Office, FO-Client): Erfassung von Anträgen durch Privatpersonen, private Organisationen oder öffentliche Stellen. Die Kommunikation erfolgt über das Internet (DMZ).
- Genehmigungsebene (Back Office, BO-Client): Erfassung (soweit nicht bereits im Front Office erfolgt), Verarbeitung der Anträge und Weiterleitung an den OSiP-Kern; Betrieb im jeweiligen Landesnetz.
- Erkenntnisebene (EKS-Client): Abruf, Prüfung und Rückmeldung sicherheitsrelevanter Erkenntnisse durch Erkenntnisstellen.

Der Datentransport zwischen diesen Ebenen erfolgt über den zentralen OSiP-Kern, in dem die Datenströme technisch validiert und für den weiteren Prozess transformiert werden. Innerhalb des Kerns werden dabei bestimmte fachliche Logiken ausgeführt, sodass Daten zeitweise im Klartext verarbeitet werden. Eine durchgängige Ende-zu-Ende-Verschlüsselung ist daher im aktuellen Betriebsmodell nicht realisiert.

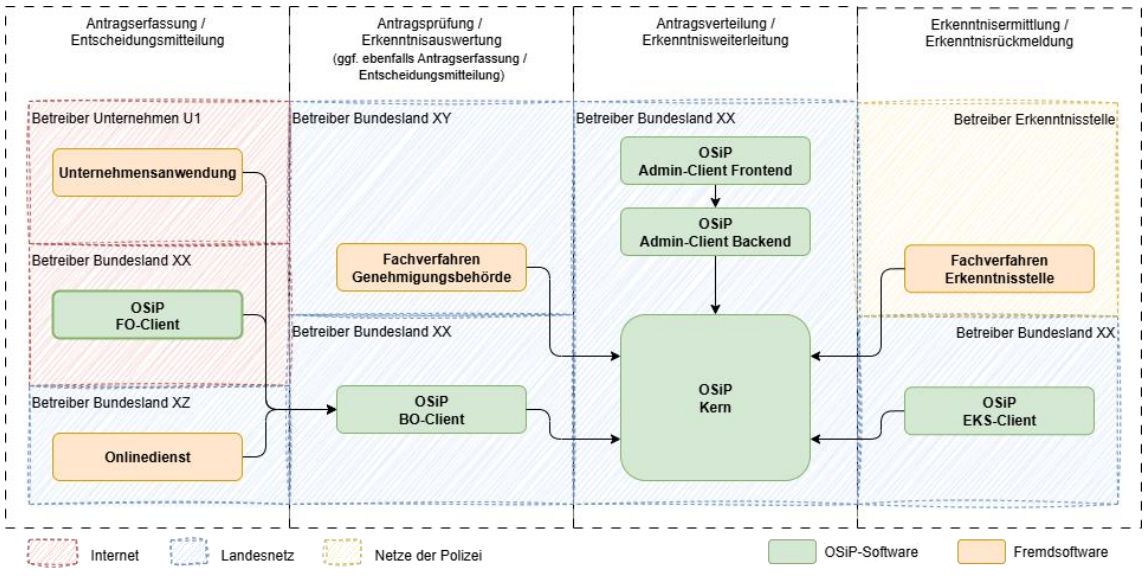


Abbildung 1

2. Prozesslogik

2.1. Genehmigung

Der Genehmigungsprozess innerhalb von OSiP umfasst mehrere standardisierte Phasen:

- Antragserfassung (durch Antragstellende oder Fachverfahren der Behörden),
- Antragsprüfung und -genehmigung durch die zuständige Genehmigungsbehörde,
- Erkenntniserhebung bei den angebundenen Erkenntnisstellen,
- Erkenntnisrückmeldung an die Genehmigungsbehörde,
- Auswertung und Entscheidungsfindung außerhalb von OSiP,
- Entscheidungsmitteilung an die betroffene Person.

Im Rahmen einer Sicherheitsüberprüfung können mehrere Landeskriminalämter (LKÄ) parallel angefragt werden. Dies erfolgt entweder manuell durch die Sachbearbeitung oder – wie im Anwendungsbereich „Luftsicherheit" – über eine automatisierte, wohnortbasierte Auswahl der anzufragenden LKÄ. In diesem Fall werden die zu beteiligenden LKÄ anhand der Wohnorthistorie (z.B. der letzten zehn Jahre) ermittelt. Voraussetzung ist, dass alle betroffenen LKÄ als Erkenntnisstelle in OSiP konfiguriert und technisch angebunden sind und die ihnen zugewiesenen Anfragen regelmäßig bearbeiten.

Rückmeldungen der Erkenntnisstellen (Erkenntnisse bzw. „keine Erkenntnis") werden grundsätzlich über denselben Kommunikationsweg an die Genehmigungsbehörde zurückgespielt; einzelne Erkenntnisstellen, insbesondere die LfV sowie weitere beteiligte Stellen, übermitteln Erkenntnisse abweichend hiervon in Papierform.

Die Systemarchitektur sieht vor, dass die Entscheidungen selbst außerhalb von OSiP getroffen und veraktet werden; das System dient ausschließlich der Datenübermittlung, nicht der Bescheiderstellung oder Zustellung.

2.2. Nachberichtspflicht

Daneben besteht für viele Anwendungsbereiche (z.B. nach dem LuftSiG oder dem WaffG) eine Nachberichtspflicht. Erkenntnisstellen sind verpflichtet, über neu hinzukommende sicherheitsrelevante Informationen innerhalb eines gesetzlich bestimmten Zeitraums unaufgefordert zu berichten. OSiP unterstützt diesen Prozess durch automatisierte Nachberichtsfunktionen, die bei neuen Erkenntnismeldungen oder Entscheidungen ausgelöst werden.

3. Anbindung und Datenaustausch

Der OSiP-Kern verwendet eigene Datenformate für den Austausch zwischen den Verfahrenskomponenten:

- AES (Antrags- und Erfassungsstruktur)
- FB (Fachbehördenstruktur)
- EKS (Erkenntnisstruktur)

Diese Formate sind OSiP-spezifisch definiert und lehnen sich nicht an bestehende XRepository-Standards an.

Im Kern erfolgt eine Transformation zwischen verschiedenen Datenformaten und Technologien, um Drittverfahren (z.B. Registersysteme wie BZR, ZStV oder GZR) anzubinden.

Die Vielzahl der angebundenen Systeme führt zu heterogenen Übertragungswegen (SOAP, REST, Dateiablagenschnittstellen). Dies erhöht die Komplexität der Kommunikationsbeziehungen und erschwert die Gewährleistung einer konsistenten IT-Sicherheit und Datenintegrität.

Anfragen an die Register werden über eine Dateischnittstelle einem Drittsystem (z.B. einer Kopfstelle zum BZR) zur Übertragung bereitgestellt. Rückmeldungen der Register werden ebenfalls über eine Dateischnittstelle in OSiP importiert.

4. Betriebsmodell und föderale Betriebsstruktur

Das Gesamtsystem wird dezentral in den Netzen der Länder und des Bundes betrieben. Jedes Land verfügt über eine eigene Instanz des OSiP-Kerns, die mit den jeweiligen Fachverfahren und Erkenntnisstellen kommuniziert.

Die Software wird zentral durch die FITKO entwickelt, die Länder sind jedoch für den operativen Betrieb, die Pflege und die Einhaltung der Sicherheitsanforderungen eigenverantwortlich zuständig.

Diese Struktur führt zu folgenden Nachteilen:

- unterschiedliche Versionsstände der OSiP-Software,
- unterschiedliche Betriebs- und Sicherheitskonzepte,
- erhöhter Wartungs- und Abstimmungsbedarf zwischen den Ländern,
- Vielzahl technischer Schnittstellen zu den Erkenntnisstellen.

Der Datenaustausch zwischen den OSiP-Instanzen der Länder und den zentralen Erkenntnisstellen (z.B. dem Bundeskriminalamt) erfolgt über den zentral betriebenen XPS3-Proxy. XPS3 fungiert als zentrale Datendrehscheibe, nimmt von den Landes-OSiP-Kernen Nachrichten entgegen, speichert sie gegebenenfalls zwischen, führt technische Prüfungen (insbesondere Format- und Plausibilitätsprüfungen) durch, adressiert sie an die jeweils zuständige Erkenntnisstelle und leitet sie dorthin weiter. Die Rückmeldungen der Erkenntnisstellen werden über denselben Weg wieder an die jeweilige Landesinstanz zurückübermittelt (siehe Abbildung 2).

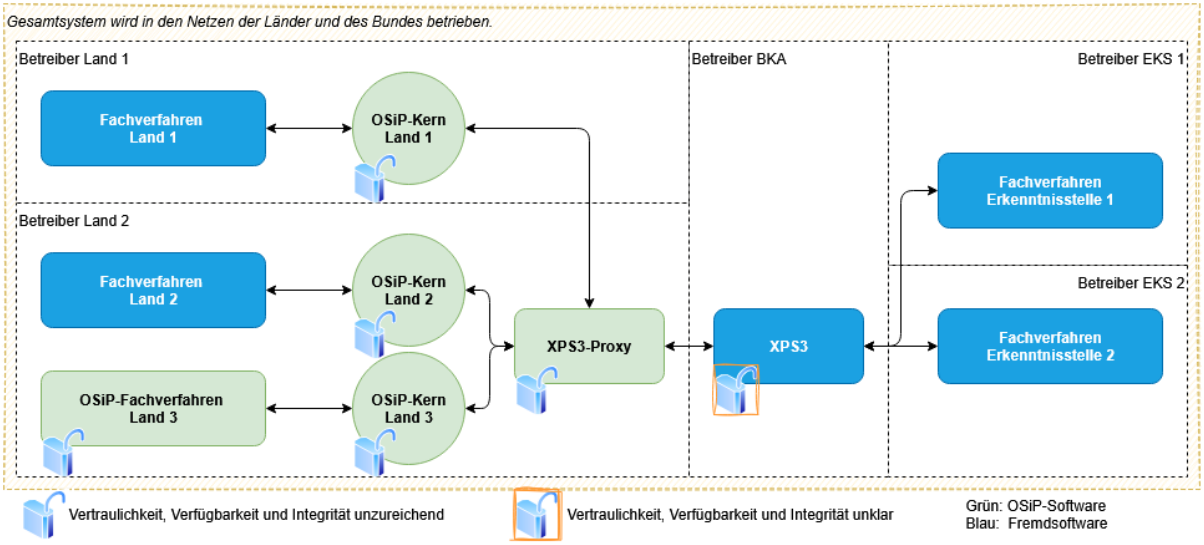


Abbildung 2

5. Technische und organisatorische Herausforderungen

Der derzeit verteilte Betrieb des OSiP-Systems führt zu einer Reihe technischer, organisatorischer und rechtlicher Herausforderungen:

- Parallele Pflege unterschiedlicher Softwareversionen mit teils inkonsistenten Updates,
- Erhöhter Wartungsaufwand und schwierige Release-Koordination zwischen Ländern und FITKO,
- Unterschiedliche IT-Sicherheitsniveaus und divergierende Datenschutzkonzepte in den Landesinstanzen,
- Fehlende Ende-zu-Ende-Verschlüsselung, da die Verarbeitung im Kern im Klartext erfolgt,
- Hohes Maß an föderaler Abstimmungsbedürftigkeit hinsichtlich Betrieb, Monitoring und Fehlerbehebung

VI. Ziele der Neukonzeption

Die FITKO arbeitet auf Grundlage des Beschlusses des IT-Planungsrats vom 26. März 2025[4] an einer grundlegenden Neukonzeption und technischen Neuentwicklung von OSiP. Ziel ist es, die bislang föderal verteilte und technisch heterogene Systemarchitektur durch ein zukunftsfähiges, einheitliches und rechtssicheres Betriebsmodell zu ersetzen, das sowohl den zentralen Datentransport als auch die Fachverfahrensunterstützung der Genehmigungsbehörden neu strukturiert.

Ein wesentlicher Teil der geplanten Reform ist die Entwicklung einer zentralen OSiP-Transportinfrastruktur, die von der FITKO betrieben und von allen Ländern gemeinsam genutzt wird. Ein mindestens ebenso wichtige Komponente ist die Neugestaltung des OSiP-Fachverfahrens als einheitliche, von der FITKO bereitgestellte Fachanwendung. Dieses Modell soll die bisherige Vielzahl an Landesinstanzen ablösen und eine konsolidierte Architektur schaffen, die den Anforderungen an Datenschutz, IT-Sicherheit und Interoperabilität gleichermaßen gerecht wird.

1. Zielarchitektur und Grundprinzipien

Der IT-Planungsrat hat die FITKO beauftragt, unter Einbeziehung der relevanten Fachbehörden und Erkenntnisstellen eine übergreifende Zielarchitektur zu entwickeln, die eine sichere, effiziente und skalierbare Durchführung von ZSÜ ermöglicht.

Kern der geplanten Architektur ist eine zentral betriebene OSiP-Transportinfrastruktur, die als Kommunikationsschicht zwischen den Fachverfahren der Länder und den Fachverfahren der Erkenntnisstellen fungiert. Entscheidungen und Bescheide werden – wie bislang – außerhalb von OSiP in den Fachverfahren getroffen und veraktet. OSiP stellt hierfür Nachrichten-, Protokoll- und Routing-Funktionen bereit.

Die Fachverfahren selbst verbleiben in der Verantwortung der Länder, während die FITKO den zentralen Transportdienst und das OSiP-Fachverfahren für Genehmigungsbehörden betreibt.

Ergänzend ist vorgesehen, auf Basis von OSiP einen zentral bereitgestellten Online-Antragsdienst zu entwickeln, über den natürliche Personen und Unternehmen Anträge elektronisch

---

[4] IT-PLR, Beschluss 2025/20 (46. Sitzung) vom 26.03.2025.

stellen können. Dieser Antragsdienst dient dem elektronischen Ausfüllen von Antragsformularen zur Übermittlung an die zuständige Behörde (vgl. § 2 Abs. 8 OZG).. Die fachliche Prüfung und Entscheidung erfolgt weiterhin in den zuständigen Fachverfahren.

Die Zielarchitektur verfolgt vier Leitziele:

- Sicherheits- und Datenschutzoptimierung: Umsetzung einer medienbruchfreien, vollständig Ende-zu-Ende-verschlüsselten Kommunikation nach den Prinzipien *Secure by Design*, *Data Protection by Design* und *Zero Trust*.
- Vereinheitlichung und Reduktion der Komplexität: Konsolidierung der bisherigen Landesinstanzen zu einem zentralen Dienst, Vereinheitlichung der Schnittstellen und Standards für Authentifizierung, Adressierung und Datenübertragung.
- Robustheit, Effizienz und Skalierbarkeit: Schaffung einer Infrastruktur, die bundesweit betreibbar, ausfallsicher und technisch erweiterbar ist.
- Homogenisierung von Schnittstellen: Erreichen einer einheitlichen Schnittstellenlandschaft für die unmittelbare Anbindung, Authentifizierung und Adressierung von Fachverfahren und Behördensystemen.

Wie und auf welchen Ebenen die Ende-zu-Ende-Verschlüsselung umgesetzt werden soll, ist derzeit noch nicht abschließend geklärt. Dies betrifft sowohl die Auswahl des kryptografischen Protokolls als auch die Umsetzungsschicht (Transport-, Anwendungs- oder Messaging-Ebene).

Wie und auf welchen Ebenen die Ende-zu-Ende-Verschlüsselung umgesetzt werden soll, ist derzeit noch nicht abschließend geklärt. Dies betrifft sowohl die Auswahl der konkreten kryptografischen Protokolle als auch die Umsetzungsschicht (Transport-, Anwendungs- oder Messaging-Ebene). Nach derzeitigem Planungsstand ist davon auszugehen, dass auf allen Kommunikationsstrecken eine abgesicherte Transportverschlüsselung nach dem Stand der Technik, voraussichtlich auf Basis von TLS mit gegenseitiger Authentifizierung (mTLS), eingesetzt wird und ergänzend ein Verfahren zur Ende-zu-Ende-Verschlüsselung der Inhaltsdaten auf Anwendungs- oder Messaging-Ebene zu spezifizieren ist. Eine Festlegung auf bestimmte Protokolle oder Standards (etwa OSCI-Transport, Messaging Layer Security (MLS) oder vergleichbare Verfahren) ist zum Zeitpunkt der Gutachtenerstellung ausdrücklich noch nicht erfolgt. Offen ist darüber hinaus, welche Metadaten in welcher Form verarbeitet werden dürfen. Nach derzeitigem Pla-

nungsstand werden voraussichtlich zumindest Informationen über Quelle, Ziel, die jeweils beteiligte Erkenntnisstelle sowie bestimmte Monitoring- und Betriebsdaten verarbeitet, um die technische Nachvollziehbarkeit und den Systembetrieb sicherzustellen.

Offen ist bislang insbesondere die Frage des Hostings der zentralen Komponenten – also, welche Betreiberorganisationen (z.B. ein Bundesrechenzentrum oder ein Landesdienstleister) den Betrieb übernehmen können und welche rechtlichen, organisatorischen und sicherheitstechnischen Anforderungen dabei einzuhalten sind. Diese Fragestellung bildet einen zentralen Gegenstand der weiteren rechtlichen Analyse dieses Gutachtens.

2. Technische Zielstruktur

Die nachfolgenden Abbildungen veranschaulichen den Aufbau und die technische Zielarchitektur der OSiP-Transportinfrastruktur. Abbildung 3 zeigt die übergeordnete Systemarchitektur mit den beteiligten Akteuren und deren Interaktion über die zentrale OSiP-Transportinfrastruktur. Abbildung 4 stellt ergänzend die technische Detailstruktur des Gesamtsystems dar, insbesondere die Anbindung der Fachverfahren und die funktionale Trennung zwischen Frontend-, Backend- und Transportkomponenten. Der „Webserver OSiP-Fachverfahren Frontend" dient ausschließlich der Auslieferung der Benutzeroberfläche an den Browser (Seitenausspielung). Fachliche Interaktionen wie Antragstellung, Datenübermittlung oder Statusabfragen erfolgen anschließend ausschließlich vom Browser zum jeweiligen Backend des Onlinedienstes.

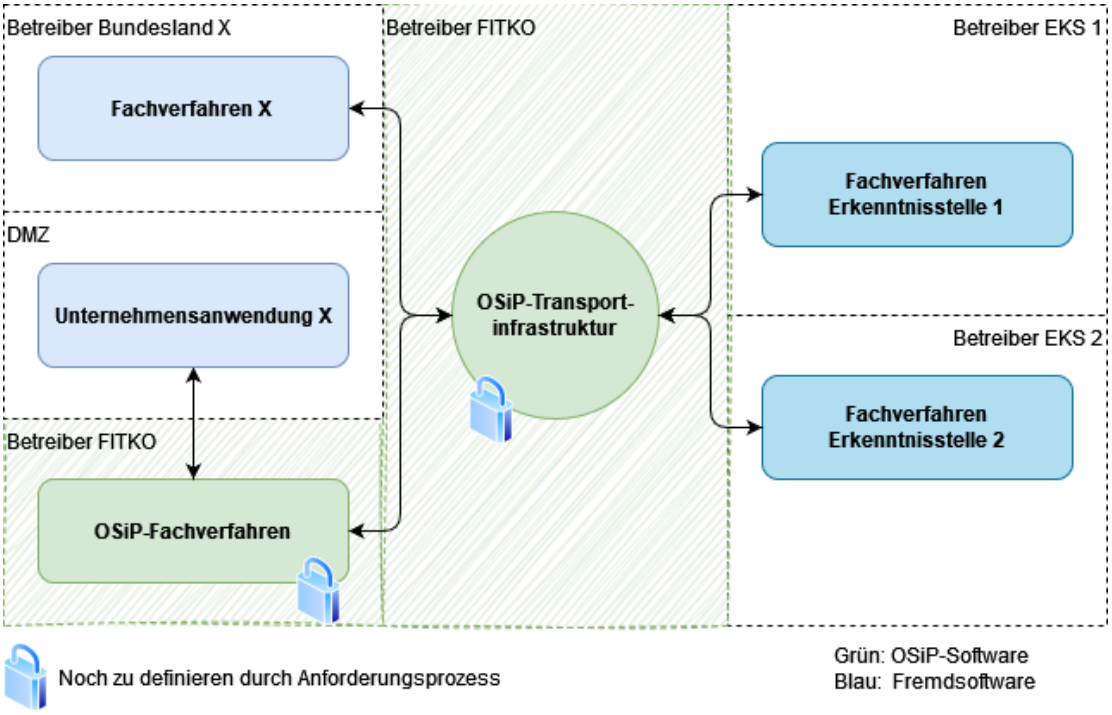


Abbildung 3

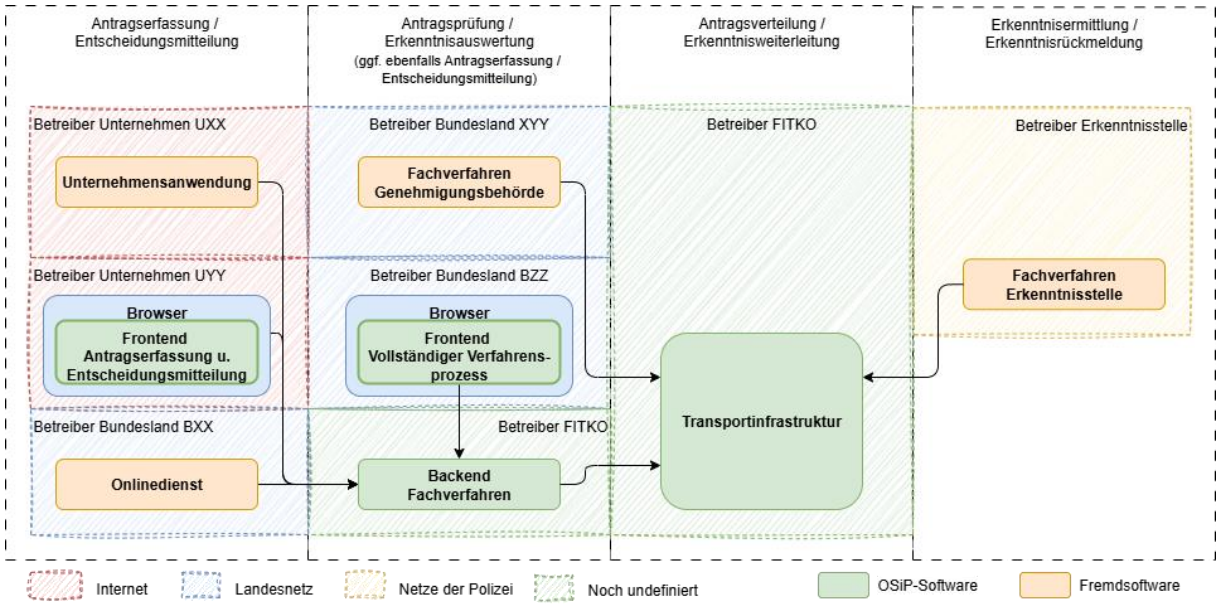


Abbildung 4

Die Abbildung verdeutlicht, dass:

- die FITKO den zentralen Transportdienst sowie das OSiP-Fachverfahren für Genehmigungsbehörden betreibt,
- die Bundesländer und Erkenntnisstellen ihre jeweiligen Fachverfahren weiterhin eigenverantwortlich führen,
- die Kommunikation über eine einheitliche, verschlüsselte Schnittstellenarchitektur erfolgt.

Damit wird die bislang dezentrale Betriebsstruktur auf eine einheitliche Kommunikations- und Sicherheitsplattform überführt.

3. Mögliche Nutzung von Adaptern

Im Bestandssystem wir derzeit ein Adapter („XPS3-Proxy“) betrieben, um Daten zwischen verschiedenen Formaten zu konvertieren, bevor sie an bzw. von verschiedenen Erkenntnisstellen weitergeleitet werden. Es ist absehbar, dass solche oder ähnliche Adapter (Format-Konverter) auch in der Zielarchitektur benötigt werden – zumindest temporär während der Migrationsphasen – um die Kompatibilität zwischen den vielfältigen Fachverfahren und den angeschlossenen Erkenntnisstellen zu gewährleisten. Ein um entsprechende Adapter erweitertes Zielbild könnte wie folgt aussehen:

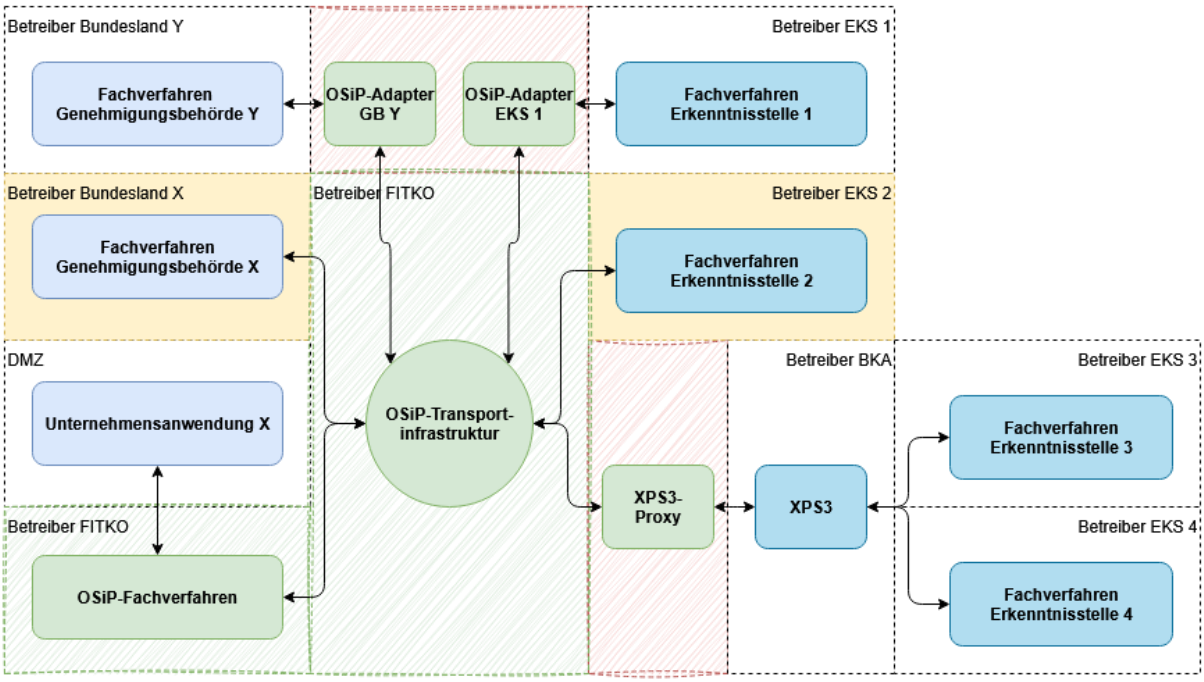


Abbildung 5

Für die Format-Konvertierung müsste eine Verschlüsselung auf dem Server, der den Adapter betreibt, vorübergehend unterbrochen werden. Dies ist unter dem Aspekt der gewünschten E2EE-Verschlüsselung relevant (siehe C.II.5.).

4. Zeitplan und Umsetzungsschritte

Nach den aktuellen Projekt- und Terminzielen (Stand 2025) sind folgende Schritte vorgesehen:

- Bis Jahresende 2025: Fertigstellung und Vorlage des Architekturkonzepts einschließlich Anforderungs- und Finanzierungsplans an den Lenkungsausschuss und das FIT-Architekturboard (FIT-AB).
- 49. Sitzung des IT-Planungsrats (2026): Beschluss über das Architektur- und Umsetzungskonzept.
- Ab 2026: Beginn der Implementierungs- und Migrationsphase in Abstimmung mit den Ländern und Erkenntnisstellen.

Die FITKO berichtet dem Lenkungsausschuss monatlich über Projektfortschritt, Risiken und strategische Entscheidungen.

C. Rechtliche Einschätzung

I. Rechtsquellen und Zuständigkeitsverteilung

1. Relevante Normen & Architekturanforderungen

Frage: „*Welche Gesetze, Verordnungen und Richtlinien auf Bundes- und Landesebene sind für Betrieb und Datennutzung relevant und was folgt daraus für die IT-Architektur des Produkts und für den Betrieb?*"

Kurzantwort:

Für OSiP ergeben sich verbindliche Architekturanforderungen aus (1.) dem Datenschutzrecht (DSGVO; BDSG/LDSG inkl. fachgesetzlicher Spezialnormen), (2.) dem IT-Sicherheitsrecht (BSIG/NIS2-Umsetzung und NIS2-UmsVO; IT-NetzG, Beschlüsse des IT-Planungsrats – insbesondere Leitlinie Informationssicherheit und Föderale IT-Architekturrichtlinie – sowie BSI-Mindeststandards) und (3.) für die Übermittlung von VS NfD aus dem Geheimschutz (SÜG/VSA Bund und Länder).

Für einzelne OSiP-Anwendungsfälle gilt die DSGVO unmittelbar (z.B. ProstSchG, Teile Luft-/Hafensicherheit) bzw. entsprechend über BDSG/LDSG. Für ZSÜ nach SÜG (Bund)/MADG greift die DSGVO nicht (da , es gelten die in § 36 SÜG genannten BDSG-Vorschriften. Auf Bundesebene konkretisieren SÜG-AVV/VSA und BSI-Vorgaben Prozesse, Nachweise und VS-IT-Eignung; auf Landesebene präzisieren VwV/VO der Landes-SÜG die Durchführung (inkl. Geheimschutz). In NRW ordnet ein OSiP-Runderlass die Nutzung von OSiP als verbindlichen Verfahrens-/Übermittlungsweg an.

Relevante Normen für die Architektur von OSiP ergeben sich aus dem Datenschutzrecht (1.1.), dem IT-Sicherheitsrecht (1.2) und – soweit durch die Erkenntnisstellen Verschlusssachen übertragen werden – den Anforderungen an den Geheimschutz (1.3).

1.1. Datenschutz

Das Datenschutzrecht dient dazu, die Grundrechte der Personen, die von einer Datenverarbeitung betroffen sind, zu schützen – insbesondere das Grundrecht auf Datenschutz bzw. „informationelle Selbstbestimmung".[5] Hierzu erlegt das Datenschutzrecht den an einer Datenverarbeitung beteiligten Akteuren Pflichten auf. Da die OSiP-Anwendungsfälle (also die Fachverfahren, in denen ZSÜ durchgeführt werden) sowie der Einsatz der Anwendung OSiP zu deren Unterstützung mit einer Verarbeitung personenbezogener Daten verbunden sind, ergeben sich aus dem Datenschutzrecht Anforderungen, die bei der Konzeption von OSiP zu beachten sind. Nachfolgend werden zunächst überblicksartig die allgemeinen Grundsätze des Datenschutzrechts (1.1.1.) und im Anschluss die konkret zu beachtenden Rechtsakte dargestellt (1.1.2.).

1.1.1. Grundzüge des Datenschutzrechts

Durch das Ineinandergreifen von EU-, Bundes- und Landesrecht und das Hinzutreten von Spezialregelungen für einzelne OSiP-Anwendungsfälle ist das auf OSiP anwendbare Datenschutzrecht komplex und auf diverse Rechtsakte verteilt (siehe 1.1.2.). Gleichwohl bleiben der Anwendungsbereich des Datenschutzrechts (1.1.1.1.), die den beteiligten Stellen zugewiesenen Rollen (1.1.1.2.) und die von ihnen zu beachtenden grundlegenden Datenschutzprinzipien (1.1.1.3.) dieselben. Diese Prinzipien sind für die Gestaltung von OSiP als IT-Anwendung der Verwaltung entscheidend und werden daher nachfolgend im Überblick dargestellt.

Die Darstellung der Prinzipien orientiert sich an der DSGVO. Diese gilt für die meisten OSiP-Anwendungsfälle unmittelbar oder entsprechend. Soweit sie für bestimmte OSiP-Anwendungsfälle nicht gilt, folgt das dann anwendbare Datenschutzrecht gleichwohl quasi identischen Prinzipien.

1.1.1.1. Anwendbarkeit des Datenschutzrechts

Voraussetzung für die Anwendbarkeit des Datenschutzrechts ist zunächst, dass überhaupt personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DSGVO). Die Begriffe „personenbezogene Daten" und „Verarbeitung" sind weit auszulegen. Somit ist eindeutig, dass im Fall von

[5] Vgl. Art. 1 DSGVO und Art. 8 EU-Charta. 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).

OSiP in den angrenzenden Fachverfahren, aber auch in der IT-Anwendung OSiP selbst, zwangsläufig personenbezogene Daten verarbeitet werden. Betroffen von der Verarbeitung (vgl. Art. 4 Nr. 1 DSGVO zur „betroffenen Person") sind jedenfalls die zu überprüfenden Personen, evtl. beteiligte Dritte (z.B. Zeugen, Kontaktpersonen) und die Nutzer der Anwendung in den Fachbehörden und Erkenntnisstellen.

1.1.1.2. Verantwortlicher und Auftragsverarbeiter

Ist mithin das Datenschutzrecht anwendbar, so sind die Datenschutzgrundsätze von allen an der Datenverarbeitung beteiligten Stellen zu beachten. Im Fall von OSiP sind dies die für ZSÜ zuständigen Fachbehörden, die Erkenntnisstellen, der die Anwendung betreibende IT-Dienstleister und die FITKO (soweit sie Daten verarbeitet oder die Verarbeitung verantwortet). Dabei unterscheidet das Datenschutzrecht zwischen der Rolle als Verantwortlicher, welcher sich dadurch auszeichnet, dass er Mittel und Zwecke der Verarbeitung bestimmt (Art. 4 Nr. 7 DSGVO) und der Rolle als Auftragsverarbeiter, der personenbezogene Daten lediglich nach Weisung verarbeitet (Art. 4 Nr. 8, Art. 28 DSGVO). An die Rollen sind unterschiedliche Pflichten geknüpft. Der Verantwortliche ist vollumfänglich für die Einhaltung des Datenschutzes verantwortlich. Der Auftragsverarbeiter muss sich an die Weisungen des Verantwortlichen halten und den technisch-organisatorischen Datenschutz gewährleisten.

Für die fachliche Durchführung der ZSÜ-Prüfungen sind die jeweils zuständigen Fachbehörden und Erkenntnisstellen als eigene Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO anzusehen. Die FITKO entscheidet insoweit nicht über Zweck und Inhalt der Prüfverfahren, sondern stellt den Ländern zentrale IT-Komponenten (Transportdienst, OSiP-Fachverfahren etc.) zur Verfügung, deren Betrieb datenschutzrechtlich grundsätzlich im Auftragsverarbeitungsmodell auszugestalten ist (mit der FITKO als Auftragsverarbeiterin und einem zentralen IT-Dienstleister gegebenenfalls als Unterauftragsverarbeiter). Unberührt bleibt, dass die FITKO für die von ihr eigenständig veranlassten Verarbeitungen (etwa im Rahmen von Produktsteuerung, Monitoring, Fehlermanagement und IT-Sicherheitsmaßnahmen) eine eigene oder gemeinsame Verantwortlichkeit mit den Ländern begründen kann (vgl. dazu unten Abschnitt II.1).

1.1.1.3. Grundsätze des Datenschutzes

Die zentralen Grundsätze, denen jede Verarbeitung personenbezogener Daten genügen muss, sind in Art. 5 Abs. 1 DSGVO zusammengefasst.[6] Die nachfolgenden Artikel der DSGVO (und weitere Gesetze wie BDSG, LDSG) konkretisieren diese Grundsätze.

1.1.1.3.1. Rechtmäßigkeit

Jede Verarbeitung personenbezogener Daten muss rechtmäßig sein, d.h. es muss einen entsprechenden Erlaubnistatbestand geben.[7] Für die OSiP-Anwendungsfälle findet sich die Erlaubnis zur Verarbeitung in einer *Rechtsgrundlage*, während die Alternativen der *Einwilligung* und des *berechtigten Interesse* im Ergebnis nicht relevant sind:

- Rechtsgrundlage: Öffentliche Stellen verarbeiten personenbezogene Daten in der Regel – und so auch im Rahmen der OSiP-Anwendungsfälle – zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 Buchst. e DSGVO). Dies muss in einer Rechtsgrundlage im Unionsrecht oder im deutschen Recht festgelegt sein (Art. 6 Abs. 3 DSGVO). Beispiel: Eine atomrechtliche Genehmigungsbehörde erhebt Erkenntnisse von einer Polizeivollzugsbehörde zum Zweck einer ZSÜ auf der Rechtsgrundlage des § 12b Abs. 3 Nr. 2 AtG.
- Einwilligung: Eine Einwilligung des Betroffenen kann zwar prinzipiell eine Rechtfertigung für eine Datenverarbeitung sein (Art. 6 Abs. 1 Buchst. a DSGVO). Bei den OSiP-Anwendungsfällen ist dies jedoch im Allgemeinen nicht der Fall, obwohl die gesetzliche Grundlage für die ZSÜ in vielen Fällen die *Zustimmung* der zu überprüfenden Person vorschreibt (vgl. § 2 Abs. 1 Satz 2 SÜG). Dieses Zustimmungserfordernis dient der Transparenz. Die Zustimmung erfüllt jedoch in der Regel nicht die Anforderungen an eine datenschutzrechtliche Einwilligung, insbesondere fehlt es regelmäßig an der dafür erforderlichen Freiwilligkeit.[8] Entscheidend für die Rechtmäßigkeit der Verarbeitung bleibt

---

[6] Für den Bereich der JI-Richtlinie siehe die Parallelnorm in Art. 4 JI-Richtlinie.

[7] Siehe Art. 5 Abs. 1 Buchst. a und Art. 6 DSGVO.

[8] Vgl. zur fehlenden Freiwilligkeit und zur ggf. sogar bestehenden Rechtspflicht zur Zustimmung *Däubler*, § 2 SÜG Rn. 11 ff. Der Hinweis von Däubler, dass § 36 Abs. 1 Nr. 2 SÜG auf § 46 Nr. 17 BDSG verweist, ist allerdings nach hier vertretener Auffassung schon deshalb irrelevant, da das SÜG gerade keine „Einwilligung" (die in § 46 Nr. 17 BDSG definiert ist), sondern eine „Zustimmung" verlangt und nicht ersichtlich ist, dass das SÜG davon ausgeht, dass beide Begriffe gleichzusetzen sind.

also die im vorigen Absatz genannte Rechtsgrundlage. Allerdings wird es an der Rechtmäßigkeit der Verarbeitung fehlen, wenn eine gesetzliche vorgeschrieben Zustimmung nicht eingeholt oder verweigert wird.[9]

- Berechtigtes Interesse: Auch auf ein berechtigtes Interesse können sich Behörden nicht berufen, um die Datenverarbeitung im Rahmen ihrer Aufgabenerfüllung zu rechtfertigen (s. Art. 6 Abs. 1 Unterabsatz 1 Buchst. f und Unterabsatz 2 DSGVO). Dieser Erlaubnistatbestand steht daher insbesondere nicht-öffentlichen Stellen zur Verfügung, kommt aber im Rahmen der OSiP-Anwendungsfälle nicht in Betracht.

Beispiel im OSiP-Kontext: Die Rechtsgrundlage für die ZSÜ im konkreten OSiP-Anwendungsfall regelt, welche Erkenntnisstellen angefragt werden können. Für freie Abfragen bei anderen Stellen fehlt es grundsätzlich an einer Rechtsgrundlage, sodass diese unzulässig sind. – Dies hängt aber im Einzelnen von den Bestimmungen des im jeweiligen OSiP-Anwendungsfall anwendbaren Fachrechts ab und kann danach für bestimmte Anwendungsfälle anders sein. So kann im Rahmen von ZSÜ nach SÜG (Bund) die mitwirkende Stelle nach § 12 Abs. 5 SÜG in ihrem Ermessen „andere geeignete Stellen befragen" oder von öffentlichen Stellen Akten beiziehen; insofern besteht dann also eine Rechtsgrundlage. Entscheidend ist, dass die Funktionalitäten im Rahmen von OSiP streng nach den jeweiligen Rechtsgrundlagen modelliert werden, um eine unzulässige Datenerhebung möglichst von vornherein zu vermeiden.

1.1.1.3.2. Zweckbindung

Personenbezogene Daten müssen zu bestimmten, legitimen Zwecken erhoben werden.[10] Im Beispiel OSiP: eine zuständige Stelle erhebt Daten von einer Erkenntnisstelle zu dem Zweck, im Rahmen ihrer gesetzlichen Aufgaben eine ZSÜ durchzuführen.

Eine Verarbeitung zu anderen Zwecken („Zweckänderung") ist grundsätzlich untersagt. Sie kommt nur in Betracht, wenn das anwendbare Fachrecht eine Weiterverarbeitung ausdrücklich vorsieht oder die Voraussetzungen des Art. 6 Abs. 4 DSGVO erfüllt sind (z. B. gesetzlich zugelassene Weiterverwendung von ZSÜ-Ergebnissen für Disziplinarverfahren). Im Beispiel OSiP be-

---

[9] *Däubler*, § 2 SÜG Rn. 14.

[10] Siehe Art. 5 Abs. 1 Buchst. b und Art. 6 Abs. 4 DSGVO.

deutet dies, dass die zuständige Stelle die erhaltenen Erkenntnisse grundsätzlich nicht an andere Stellen weiterübermitteln oder für Zwecke verwenden darf, die außerhalb der ursprünglichen ZSÜ liegen.

1.1.1.3.3. Treu und Glauben

Die Anforderung aus Art. 5 Abs. 1 Buchst. a DSGVO, dass die Verarbeitung personenbezogener Daten nach Treu und Glauben erfolgen muss, ist sehr abstrakt und soll an dieser Stelle nicht weiter vertieft werden.

1.1.1.3.4. Transparenz

Wichtig für die Gestaltung von Verarbeitungsverfahren ist der Grundsatz der Transparenz, also der Nachvollziehbarkeit für die betroffenen Personen. Diese gesetzliche Anforderung der Transparenz mündet bei der Gestaltung von IT-Systemen u.a. in Erfordernissen zur Protokollierung von Verarbeitungsvorgängen sowie in Funktionen, die die Umsetzung der Betroffenenrechte auf Information (Art. 13, 14 DSGVO), auf Auskunft (Art. 15 DSGVO) und darauf aufbauend auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO) ermöglichen.

Im Kontext von ZSÜ ist zu beachten, dass diese Rechte häufig spezialgesetzlich eingeschränkt sind oder sich der Umfang des Auskunftsrechts überhaupt vollständig nach dem Spezialgesetz richtet. So gilt bei Überprüfungen nach dem SÜG des Bundes (einschließlich von Überprüfung nach Gesetzen, die auf das SÜG verweisen) für das Auskunftsrecht einer betroffenen oder mitbetroffenen Person gegen die für eine ZSÜ zuständige oder daran mitwirkende Behörde die Regelung des § 23 SÜG. Diese Regelung basiert zwar auf dem datenschutzrechtlichen Transparenzprinzip, sie enthält aber in § 23 Art. 2-5 SÜG ganz erhebliche Einschränkungen des Auskunftsrechts zugunsten von Sicherheitsbelangen und Quellenschutz. Zwar sind diese Belange gegen das Interesse der anfragenden Person abzuwägen (siehe § 23 Abs. 3 SÜG), jedoch werden die Sicherheitsbelange vielfach Vorrang erhalten.[11] Im Ergebnis können daher unter anderem Auskunftsanfragen, die sich auf mit OSiP übermittelte Informationen von Erkenntnisstellen richten (z.B. verdeckte Erkenntnisse von BfV, LfV oder LKA), je nach den Umständen abzulehnen sein um laufende Ermittlungen, nachrichtendienstliche Arbeitsweisen oder sonstige Sicherheits-

[11] Kritisch Däubler, SÜG § 23 Rn. 1.

belange nicht zu gefährden. OSiP sollte daher entsprechende Kennzeichnungen von Erkenntnissen durch die Erkenntnisstellen zulassen, systemseitig abbilden und bei Auskunfts-, Export- und Protokollfunktionen berücksichtigen. Auskunftsansprüche müsse aber letztlich von der angefragten Behörde im Einzelfall geprüft und beschieden werden.

In der Zielarchitektur stellt das OSiP-Fachverfahren-Backend nur die erforderlichen technischen Funktionen zur Verfügung, insbesondere zur Anzeige, Änderung, Sperrung, zum Export und zur Löschung von Datensätzen unter Beachtung der Ende-zu-Ende-Verschlüsselung. Die organisatorische Umsetzung der Betroffenenrechte, z.B. die Entgegennahme und Prüfung von Anträgen, Prüfung gesetzlicher Ausschlussgründe (etwa bei verdeckten Erkenntnissen), Entscheidung und Dokumentation, obliegt den datenschutzrechtlich Verantwortlichen.

1.1.1.3.5. Datenminimierung (Erforderlichkeit)

Die Verarbeitung personenbezogener Daten muss „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein".[12] Einfacher gesagt dürfen nur die Daten erhoben werden, die zur Erreichung des festgelegten Verarbeitungszwecks „erforderlich" sind.[13] Die Forderung, Daten auf das notwendige Maß zu beschränken, bedeutet, dass personenbezogene Daten nicht einfach deshalb erhoben und verarbeitet werden dürfen, weil sie nützlich sind und die Zweckerreichung fördern („angemessen und erheblich"). Vielmehr muss geprüft werden, ob der Zweck nicht auch ohne diese Daten, mit aggregierten oder anonymisierten Daten oder mit einem Weniger an Daten erreicht werden kann.[14] Der Grundsatz der Datenminimierung wird an verschiedenen Stellen in der DSGVO aufgegriffen, er ist insbesondere auch im Rahmen von „Privacy by Design" (Art. 25 DSGVO), also bei der Gestaltung von IT-Verfahren und -Systemen zu berücksichtigen.

Beispiel im OSiP-Kontext: Das Generieren von Pseudonymen stellt eine Verarbeitung personenbezogener Daten da. Werden Daten von natürlichen Personen verarbeitet, so ist es IT-technisch üblich und regelmäßig unvermeidbar, dass einzelnen natürlichen Personen programmintern bei der Speicherung in einer Datenbank IDs (z.B. Datensatz-Schlüssel, UUIDs) zugeordnet werden. Die Verarbeitung muss insofern jedoch datensparsam bleiben. D.h., die IDs dürfen grundsätzlich

---

[12] Art. 5 Abs. 1 Buchst. c DSGVO.

[13] Herbst in Kühling/Buchner, 4. Aufl., Art. 5 DSGVO Rn. 57.

[14] Herbst in Kühling/Buchner, 4. Aufl., Art. 5 DSGVO Rn. 57.

nicht exportiert und für andere Zwecke als die interne Datenverarbeitung verwendet werden. Sie dürfen z.B. nicht – jedenfalls nicht ohne eindeutige Rechtsgrundlage – für außerhalb des eigentlichen Verarbeitungszwecks liegende Zwecke genutzt werden, wie etwa für einen mandantenübergreifenden Dublettenabgleich oder das Anlegen eines gesetzlich nicht vorgesehenen „Schattenregisters" von Personen, die im Rahmen einer ZSÜ überprüft wurden oder zu denen Erkenntnisse vorliegen.

1.1.1.3.6. Richtigkeit

Daten müssen im Hinblick auf den Verarbeitungszweck richtig und aktuell sein. Wenn dies nicht gegeben ist, bestehen ggf. Pflichten zur Berichtigung (vgl. Art. 16 DSGVO) oder zur Löschung (vgl. Art. 17 Abs. 1 Buchst. d DSGVO). Bei der Gestaltung von Verarbeitungsverfahren sind Maßnahmen zu treffen, damit diese Pflichten bei Bedarf erfüllt, also Daten berichtigt oder gelöscht werden können.

1.1.1.3.7. Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die Verarbeitungszwecke erforderlich ist.[15] Es bedarf daher in der Praxis eines Löschkonzeptes, d.h. einer Definition von Löschfristen für sämtliche personenbezogenen Daten, die sich aus der Erforderlichkeit der Daten für die verfolgten Verarbeitungszwecke und ggf. hinzutretenden gesetzlichen Anforderungen (z.B. Aufbewahrungsfristen) ableiten. Entsprechende Löschroutinen müssen in IT-Anwendungen konfigurierbar und automatisch ausführbar und die Löschvorgänge müssen nachweisbar sein.

1.1.1.3.8. Datensicherheit

Bei der Verarbeitung personenbezogener Daten muss deren Sicherheit gewährleistet werden;[16] siehe hierzu auch Art. 32 DSGVO. Die klassischen Schutzziele der Datensicherheit umfassen zunächst die klassischen Schutzziele der IT-Sicherheit, nämlich

- Vertraulichkeit (Schutz gegen unbefugten Zugriff),

---

[15] Herbst in Kühling/Buchner, 4. Aufl., Art. 5 DSGVO Rn. 57

[16] Vgl. Art. 5 Abs. 1 Buchst. e DSGVO.

- Integrität (Unversehrtheit von Daten und Systemen; Erkennbarkeit von Veränderungen) und
- Verfügbarkeit

von IT-Systemen und Daten.[17] Diese Ziele werden in der DSGVO ausdrücklich genannt. Es lassen sich jedoch noch weitere Schutzziele aus der DSGVO ableiten, die ebenfalls elementare Ziele der IT-Sicherheit sind:

- Authentizität (Verbindlichkeit und Herkunftssicherheit von Nachrichten, Dokumenten und Urkunden),[18]
- Revisionsfähigkeit bzw. Revisionssicherheit (die Fähigkeit, dass jederzeit festgestellt werden kann, wer wann welche Daten in welcher Weise verarbeitet hat),[19]

Schließlich werden aus datenschutzrechtlicher Sicht weitere Schutzziele gefordert, die über die herkömmliche IT-Sicherheit hinausgehen und darauf gerichtet sind, die Einhaltung des materiellen Datenschutzrechts zu ermöglichen und zu fördern. Insoweit sind Verantwortliche über Art. 24 DSGVO, der sich über die Datensicherheit hinaus auf die Einhaltung der materiellen Vorgaben der DSGVO insgesamt richtet, zu entsprechenden Maßnahmen verpflichtet. Dies zu gewährleistenden Datenschutz-Ziele, die etwa auch im Standard-Datenschutz-Modell (SDM) der Aufsichtsbehörden gefordert werden, sind:[20]

- Transparenz (s.o. 1.1.1.3.4.)
- Nichtverkettbarkeit (Erschwerung einer zweckwidrigen Auswertung in Verbindung mit weiteren Daten/Hintergrundwissen)
- Intervenierbarkeit (Ermöglichung der Geltendmachung von Betroffenenrechten) sowie
- Datenminimierung (s.o. 1.1.1.3.5)

1.1.1.4. Rechenschaftspflicht

Eine Art „Meta-Grundsatz" stellt die Rechenschaftspflicht dar (Art. 5 Abs. 2 DSGVO). Danach sind die Verantwortlichen für die Einhaltung der Datenschutzgrundsätze (1.1.1.3) zuständig und

---

[17] Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 5.

[18] Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 6.

[19] Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 7.

[20] Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 8.

müssen die Einhaltung nachweisen können. Bei IT-gestützter Verarbeitung ergeben sich hieraus für das Design von IT-Systemen entsprechende Anforderungen an die Gewährleistung der Nachvollziehbarkeit und Beweisbarkeit, was u.a. in konkrete Maßnahmen zur Sicherstellung von Integrität und Authentizität und in die notwendige Protokollierung von Verarbeitungsvorgängen mündet.

1.1.1.5. Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

Das Prinzip des Datenschutzes durch Technikgestaltung (Art. 25 DSGVO) – englisch „Data Protection by Design" oder „Privacy by Design" – konkretisiert den Auftrag an den Verantwortlichen, bereits in der Gestaltungsphase der Verarbeitung geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um die Datenschutzgrundsätze (1.1.1.3) umzusetzen. Bei einer IT-gestützten Verarbeitung wie OSiP müssen also bereits in der Konzeptionsphase solche Maßnahmen systematisch geprüft und ausgewählt werden.

Wie auch sonst in der DSGVO wird dabei ein risikobasierter Ansatz vorgegeben.[21] Das bedeutet, dass auf Grundlage einer Risikoanalyse, die die typischen und vorhersehbaren Risikoszenarien erfasst und abdeckt, die angemessenen TOM auszuwählen und zu implementieren sind. Bei der Maßnahmenauswahl sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie das Ausmaß der Risiken (Eintrittswahrscheinlichkeit und Schwere) zu berücksichtigen.

1.1.1.6. Umsetzung des Datenschutzes beim Design von IT-Systemen

Die gesetzlichen formulierten Anforderungen an die Datensicherheit (Art. 32 DSGVO) und an Datenschutz durch Technikgestaltung (Art. 25 DSGVO) geben weitgehend sehr abstrakte Ziele vor, die bei der Umsetzung konkretisiert werden müssen. Dies gilt für das Datenschutzrecht ebenso wie für das Recht der IT-Sicherheit. Verlangt wird ein „risikoangemessenes Sicherheitsniveau".

In Art. 25 und 32 DSGVO, aber auch vielen anderen gesetzlichen Vorgaben, wird die Berücksichtigung des „Standes der Technik" eingefordert. Dies verweist nach ständiger Rechtsprechung auf anerkannte Normen und Standards, die mithin in der Praxis heranzuziehen sind. So kann und sollte für konkrete Fragen der IT-Sicherheit auf Technischen Richtlinien des BSI (z.B. TR-02102-1 zur Kryptografie etc.) zurückgegriffen werden und für ein Sicherheitskonzept im

[21] Vgl. Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 22 ff.

Allgemeinen auf den IT-Grundschutz des BSI (der seinerseits auf der ISO2700x-Normreihe beruht). Für eine spezifisch datenschutzrechtlich motivierte Herangehensweise kann das Standard-Datenschutz-Modell herangezogen werden.

Das konkret für OSiP geltende Datenschutzrecht (1.1.2.) verweist zum Teil auf konkrete Regelwerke – insbesondere die Vorgaben des BSI, aber auch auf das SDM. Zum Teil werden die umzusetzenden Maßnahmen auch im Gesetz selbst oder in darauf aufbauenden untergesetzlichen Normen (z.B. Beschlüssen des IT-Planungsrats und Verwaltungsvorschriften) konkretisiert. Die relevanten Normen werden im Folgenden Abschnitt genannt.

1.1.2. Anwendbares Datenschutzrecht

Zu berücksichtigen sind die Datenschutzregelungen der EU, des Bundes und der Länder.

Die wichtigste Regelung zum Datenschutz auf EU-Ebene ist die DSGVO. Im Ergebnis ist sie auf fast alle OSiP-Anwendungsfälle anwendbar. Allerdings gilt die DSGVO nur zum Teil unmittelbar und im Übrigen mittelbar über eine Verweisung aus dem BDSG bzw. den LDSG. Weder unmittelbar noch mittelbar unter die DSGVO fallen allerdings die OSiP-Anwendungsfälle „SÜG (Bund)“ und MADG. Siehe im Einzelnen 1.1.2.1.

Auf Bundesebene gilt für die Datenverarbeitung durch die Bundesbehörden grundsätzlich das BDSG. Für die OSiP-Anwendungsfälle sind außerdem die speziellen Regelungen zum Datenschutz in den jeweiligen Rechtsgrundlagen für die ZSÜ zu beachten. Siehe 1.1.2.2.

Entsprechendes gilt für die Landesebene: Während die Datenverarbeitung durch Landesbehörden – unabhängig davon, ob Bundes- oder Landesrecht ausgeführt wird – grundsätzlich unter das LDSG fällt, sind ggf. die datenschutzrechtlichen Spezialregelungen in den jeweiligen ZSÜ-Rechtsgrundlagen zu beachten. Siehe 1.1.2.2.2.

1.1.2.1. EU (DSGVO)

Die EU ist zur Regelung des Datenschutzes befugt hinsichtlich von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen (Art. 16 Abs. 2 AEUV). Diese Gesetzgebungsbefugnis wurde insbesondere ausgeübt durch Erlass der DSGVO.[22] Die DSGVO gilt grundsätzlich für jede

[22] Außerdem sind zu nennen: die JI-Richtlinie (Richtlinie (EU) 2016/680) über den Datenschutz im Bereich von Justiz und Strafverfolgung sowie die Verordnung (EU) 2018/1725 über den Datenschutz im Bereich der EU-Organe.

Verarbeitung personenbezogener Daten. Sie regelt daher auch die meisten OSiP-Anwendungsfälle unmittelbar. Es gibt jedoch zwei wichtige Ausnahmen vom Anwendungsbereich der DSGVO, von denen eine insbesondere die nationale Sicherheit betrifft (vgl. Art. 2 Abs. 2 Buchst. a DSGVO) und die andere Tätigkeiten im Bereich Justiz, Strafverfolgung und Strafvollzug (Art. 2 Abs. 2 Buchst. d DSGVO). Diese Ausnahmen sind also für jeden der OSiP-Anwendungsfälle zu prüfen, um zu ermitteln, ob die DSGVO jeweils *unmittelbar* Anwendung findet (siehe 1.1.2.1.1).

Soweit die DSGVO nicht unmittelbar Anwendung findet, gilt sie in vielen Fällen im Ergebnis dennoch. Denn das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze (LDSG) verweisen in diesen Fällen grundsätzlich auf die DSGVO und erklären sie für entsprechend anwendbar (siehe 1.1.2.1.2).

Für eine tabellarische Übersicht über die Anwendung der DSGVO in den verschiedenen Anwendungsfällen siehe II.

1.1.2.1.1. Unmittelbare Anwendbarkeit der DSGVO

Die DSGVO gilt, soweit personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DSGVO).

Eine relevante Ausnahme sind Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (Art. 2 Abs. 2 Buchst. a DSGVO). Dies gilt insbesondere für den Bereich „nationale Sicherheit", dem einige der OSiP-Anwendungsfälle zuzuordnen sind. Für einen Teil dieser Fälle scheidet deshalb die Anwendung der DSGVO aus (siehe 1.1.2.1.1.1.).

In den meisten OSiP-Anwendungsfällen, die dem Bereich der nationalen Sicherheit zuzuordnen sind, gilt die DSGVO aber im Ergebnis gleichwohl entweder unmittelbar oder entsprechend (siehe 1.1.2.1.1.2.).

Die zweite relevante Ausnahme sind Tätigkeiten, die der Justiz, dem Strafvollzug oder der Strafvollstreckung zuzuordnen sind (Art. 2 Abs. 2 Buchst. d DSGO). Hierfür gilt die DSGVO jedenfalls nicht unmittelbar. Stattdessen gelten die Datenschutzvorschriften des jeweiligen Landes- oder Bundesrechts, die jedoch teils wieder auf die DSGVO verweisen (siehe 1.1.2.1.1.3).

In den übrigen OSiP-Anwendungsfällen gilt die DSGVO unmittelbar (siehe 1.1.2.1.1.4).

1.1.2.1.1.1. OSiP-Anwendungsfälle im Bereich „nationale Sicherheit", die nach Art. 2 Abs. 2 Buchst. a DSGVO nicht unter die DSGVO fallen

Nicht in den Anwendungsbereich des Unionsrechts – und damit nicht unter die DSGVO – fallen Tätigkeiten, die der Wahrung der nationalen Sicherheit dienen oder die „derselben Kategorie zugeordnet werden können".[23] Somit ist für jeden Anwendungsfall von OSiP zu prüfen, ob Zwecke der „nationalen Sicherheit" verfolgt werden; denn in diesem Fall ist die DSGVO nach Art. 2 Abs. 2 Buchst. a DSGVO nicht unmittelbar anwendbar.

Der nationalen Sicherheit dienen insbesondere solche Tätigkeiten, die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken.[24] Zur nationalen Sicherheit dürfte damit etwa die Sabotage- und Terrorabwehr gehören. Ein Gegenbeispiel sind Tätigkeiten, die alltäglichere Sicherheitsinteressen betreffen, wie die Straßenverkehrssicherheit.[25]

Nach dem genannten Maßstab fallen Sicherheitsüberprüfungen nach SÜG (Bund) in die Kategorie der nationalen Sicherheit.[26] Folglich sind diese von der unmittelbaren Anwendung der DSGVO umfassend ausgenommen. Zwar ist Art. 2 Abs. 2 Buchst. a DSGVO als Ausnahmevorschrift eng auszulegen.[27] Innerhalb der unter das SÜG fallenden Tätigkeiten, die der nationalen Sicherheit dienen, gilt die Ausnahme aber umfassend. Somit ist etwa eine nach SÜG geführte Sicherheitsakte von der Anwendbarkeit der DSGVO ausgenommen, und zwar auch, soweit darin enthaltene personenbezogene Daten für andere Zwecke (z.B. Disziplinarverfahren, beamtenrechtliche Auswahlentscheidungen etc.) genutzt worden sind und ohne dass im Einzelfall zu prüfen ist, ob alle in der Akte verarbeiteten personenbezogenen Daten einen direkten Bezug zur Sicherheit des Staats haben.[28]

Die Ausnahme des Art. 2 Abs. 2 Buchst. a DSGVO gilt ferner für ZSÜ nach dem MADG, die nach den Vorschriften des SÜG durchgeführt werden. Auch darauf ist die DSGVO nicht anwendbar.

---

[23] Vgl. Art. 2 Abs. 2 Buchst. a und Erwägungsgrund 16 DSGVO; EuGH, Urt. v. 22.06.2021, Az. C-439/19 Rn. 66; Bäcker in BeckOK DSR, 53. Ed., Art. 2 DSGVO Rn. 9.

[24] EuGH, Urt. v. 22.06.2021, Az. C-439/19 Rn. 67.

[25] EuGH, Urt. v. 22.06.2021, Az. C-439/19 Rn. 68.

[26] OVG NRW, Beschluss v. 28.07.2021, Az. 16 B 1733/19 [= ZD 2022, 67], Rn. 8.

[27] EuGH, Urt. v. 22.06.2021, Az. C-439/19 Rn. 62.

[28] OVG NRW, Beschluss v. 28.07.2021, Az. 16 B 1733/19 [= ZD 2022, 67], Rn. 8.

1.1.2.1.1.2. OSiP-Anwendungsfälle im Bereich „nationale Sicherheit", in denen dennoch die DSGVO gilt

Eine Reihe von OSiP-Anwendungsfällen dient zwar (auch) der nationalen Sicherheit – so dass Art. 2 Abs. 2 Buchst. a DSGVO zu prüfen ist –, jedoch ist im Ergebnis die DSGVO gleichwohl entweder unmittelbar oder entsprechend anwendbar.

Dies betrifft zunächst ZSÜ nach Luftsicherheitsrecht und Hafensicherheitsrecht. Diese dienen zwar u.a. der nationalen Sicherheit, jedoch ist für Seeschifffahrt und Luftfahrt nach Art. 100 Abs. 2 AEUV der Anwendungsbereich des Unionsrecht eröffnet und es bestehen unionsrechtliche Grundlagen für die Prüfungen. Somit greift die Ausnahme des Art. 2 Abs. 2 Buchst. a DSGVO nicht ein und es bleibt bei der unmittelbaren Anwendung der DSGVO.

Zuverlässigkeitsprüfungen nach § 12b AtomG dienen ebenfalls der nationalen Sicherheit. Teilweise sind hierfür Regelungen auf Basis des Euratom-Vertrages zu beachten. Es ist nicht eindeutig, ob damit für die Prüfung der „Anwendungsbereich des Unionsrechts" im Sinne von Art. 2 Abs. 2 Buchst. a DSGVO eröffnet ist – also ob die DSGVO unmittelbar gilt. Jedenfalls ist die DSGVO aber entsprechend anwendbar über die Verweise der LDSG bzw. des BDSG.

Schließlich wird auch in den OSiP-Anwendungsfällen Sprengstoffrecht, Waffenrecht, Jagdrecht, Bewachungsgewerbe und Einbürgerungs- und Aufenthaltsrecht (auch) der Zweck der nationalen Sicherheit verfolgt. In allen diesen Fällen muss also in Betracht gezogen werden, dass die DSGVO ggf. nach Art. 2 Abs. 2 Buchst. a DSGVO nicht unmittelbar anwendbar ist. Allerdings ist in diesen Fällen die DSGVO über die Verweise der LDSG bzw. des BDSG entsprechend anwendbar.

1.1.2.1.1.3. OSiP-Anwendungsfälle im Bereich Justiz und Strafverfolgung (Art. 2 Abs. 2 Buchst. d DSGVO)

Nach Art. 2 Abs. 2 Buchst. d DSGVO ist die DSGVO auf Tätigkeiten im Bereich der Justiz und Strafverfolgung (einschließlich Strafvollzug) nicht anzuwenden. Für diesen Bereich ist der Datenschutz auf EU-Ebene in der JI-Richtlinie geregelt, die als EU-Richtlinie nicht unmittelbar gilt, sondern in mitgliedstaatliches Recht umgesetzt ist.

Die Ausnahme ist vorliegend relevant für die OSiP-Anwendungsfälle „Justizvollzug" und ggf. „Anlassbezogene Überprüfungen". Damit gilt für diese Anwendungsfälle die DSGVO nicht unmittelbar. Stattdessen gelten das jeweilige LDSG bzw. die speziellen Datenschutzvorschriften im Fachrecht (z.B. JVollzDSG NRW).

Soweit die LDSG für den Bereich der Justiz und der Strafverfolgung auf die DSGVO verweisen (was zum Teil der Fall ist), gilt die DSGVO in den genannten OSiP-Anwendungsfällen entsprechend (siehe im Einzelnen II).

1.1.2.1.1.4. OSiP-Anwendungsfälle, die unmittelbar unter die DSGVO fallen

Soweit die OSiP-Anwendungsfälle weder dem Bereich nationale Sicherheit noch dem Bereich Justiz/Strafverfolgung zuzuordnen sind, bleibt es bei der unmittelbaren Anwendbarkeit der DSGVO. Dies gilt etwa für Zuverlässigkeitsprüfungen nach ProstSchG.

1.1.2.1.2. Entsprechende Anwendbarkeit

Fällt eine Tätigkeit nicht in den Anwendungsbereich des Unionsrechts und damit nach Art. 2 Abs. 2 Buchst. a DSGVO nicht unmittelbar unter die DSGVO, so gilt zunächst nationales Datenschutzrecht. Die Datenschutzgesetze des Bundes und der Länder ordnen in diesem Fall jedoch grundsätzlich die entsprechende Geltung der DSGVO an.[29] Somit gilt die DSGVO – auf dem Umweg über BDSG/LDSG – im Ergebnis grundsätzlich auch für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, einschließlich von Tätigkeiten im Bereich der nationalen Sicherheit.

Zu beachten ist jedoch, dass die eben genannte Verweisung von BDSG/LDSG auf die DSGVO für Sicherheitsüberprüfungen teilweise spezialgesetzlich wieder eingeschränkt oder ausgeschlossen wird. Für OSiP-Anwendungsfälle, die unter Art. 2 Abs. 2 Buchst. a DSGVO fallen (siehe 1.1.2.1.1.1 und 1.1.2.1.1.2), ist daher jeweils zu prüfen, ob es besondere Vorschriften gibt, die die Geltung der DSGVO regeln.

Zum Beispiel ergibt sich für die Sicherheitsüberprüfung nach SÜG (Bund), dass § 36 Abs. 1 Nr. 1 SÜG die Geltung von § 1 Abs. 8 BDSG – und damit die entsprechende Anwendung der DSGVO – ausschließt. Vielmehr sind in diesem Fall nur die in § 36 SÜG (Bund) genannten Vorschriften des BDSG anwendbar.

---

[29] Siehe § 1 Abs. 8 BDSG; § 2 Abs. 4 Nr. 1 LDSG BW; Art. 2 Satz 1 BayDSG; § 2 Abs. 9 BlnDSG; § 2 Abs. 6 BbgDSG; § 2 Abs. 6 Satz 1 BremDSGVOAG; § 2 Abs. 6 HmbDSG; § 1 Abs. 8 HDSIG; § 1 Abs. 2 DSG M-V (unklar); § 2 Nr. 2 Buchst. c NDSG; § 5 Abs. 8 Satz 1 DSG NRW; § 10 LDSG R-P; § 3 Abs. 1 DSG SL; § 2 Abs. 4 SächsDSDG; § 3 Abs. 2 DSAG LSA; § 2 Abs. 6 LDSG S-H; § 2 Abs. 4 Satz 1 ThürDSG.

1.1.2.2. Bund

Grundsätzlich wird die Datenverarbeitung durch deutsche Behörden durch die DSGVO geregelt. Soweit die DSGVO nicht anwendbar ist – insbesondere im Bereich der nationalen Sicherheit oder der JI-Richtlinie (siehe im Einzelnen 1.1.2.1.) – oder Öffnungsklauseln enthält, kann der deutsche Gesetzgeber den Datenschutz regeln. Ob innerstaatlich der Bund oder das Land zuständig ist, bestimmt sich nach den im Grundgesetz zugewiesenen Gesetzgebungskompetenzen. Der Bund ist zuständig für das Verwaltungsverfahren der Bundesbehörden und damit auch für die Datenverarbeitung durch die Bundesbehörden im Rahmen_ihrer Aufgabenerfüllung. Hierfür gilt grundsätzlich das BDSG (1.1.2.2.1). Das dem jeweiligen OSiP-Anwendungsfall zugrunde liegende Fachrecht enthält jedoch regelmäßig die datenschutzrechtliche Rechtsgrundlage für die Verarbeitung und zum Teil auch weitergehende datenschutzrechtliche Regelungen (1.1.2.2.2). Zudem sind datenschutzrechtliche Anforderungen ggf. in untergesetzlichen Regelungen enthalten (1.1.2.2.3).

1.1.2.2.1. BDSG

1.1.2.2.1.1. Grundsatz: Geltung des BDSG für Bundesbehörden

Soweit nicht die DSGVO gilt (siehe 1.1.2.1.), fällt die Datenverarbeitung durch Bundesbehörden grundsätzlich unter das BDSG (§ 1 Abs. 1 Nr. 1 BDSG). Hierzu gehört auch die Tätigkeit der Bundesbehörden im Rahmen der OSiP-Anwendungsfälle, soweit sie

- als zuständige Behörde eine Zuverlässigkeits- oder Sicherheitsüberprüfung durchführen oder
- als Erkenntnisstelle oder sonst an dem Verfahren beteiligt sind.

1.1.2.2.1.2. Ausnahme: Spezialregelungen oder Ausschluss der Anwendung des BDSG

Zu beachten ist, dass die für den OSiP-Anwendungsfall geltenden Rechtsgrundlagen zum Teil Spezialregelungen zum Datenschutz enthalten, die dem BDSG vorgehen oder dieses ggf. sogar ganz verdrängen (siehe 1.1.2.2.2.). Ferner wird die Geltung des BDSG auch ausdrücklich eingeschränkt.

Ein Beispiel für beides – d.h. für eine vorrangige Spezialregelung und einen ausdrücklichen Ausschluss des BDSG – ist der Anwendungsfall „SÜG (Bund)". Das SÜG (Bund) enthält eigene Regelungen zum Datenschutz, die nach Ansicht des Gesetzgebers ein „bereichsspezifisches Datenschutzvollsystem" darstellen.[30] Durch diese detaillierte Regelung soll das BDSG als Ganzes verdrängt werden.[31] Klargestellt wird das durch § 36 SÜG, der § 1 Abs. 8 BDSG und damit die Anwendung des BDSG insgesamt ausschließt. Stattdessen gelten für den Anwendungsfall „SÜG (Bund)" die Spezialregelungen zum Datenschutz im SÜG selbst sowie diejenigen Vorschriften des BDSG, deren entsprechende Geltung in § 36 Abs. 1 Nr. 2 SÜG angeordnet wird. Insbesondere sind danach die Regelungen zur Auftragsverarbeitung (§ 62 BDSG) und zur Datensicherheit (§ 64 BDSG) auch im Bereich des SÜG entsprechend anzuwenden (nicht aber z.B. die besonderen Bedingungen zur Datenübermittlung nach § 74 BDSG).

1.1.2.2.1.3. Teil 2 (Ergänzung der DSGVO) vs Teil 3 (Umsetzung der JI-Richtlinie)

Bei Anwendung des BDSG im Falle von OSiP ist zu beachten, dass unterschiedliche Teile des Gesetzes für unterschiedliche OSiP-Anwendungsfälle relevant sein können:

- Teil 2 des BDSG (§§ 22 bis 44 BDSG) enthält für Fälle, die unter die DSGVO fallen, ergänzende Regelungen, die die Öffnungsklauseln der DSGVO ausfüllen.
- Teil 3 des BDSG (§§ 45 bis 84 BDSG) ist anwendbar, sofern öffentliche Stellen zu Zwecken der Strafverfolgung und des Strafvollzugs personenbezogene Daten verarbeiten (§ 45 BDSG). Hierauf ist die DSGVO nicht anwendbar, vielmehr fällt dieser Bereich unter die JI-Richtlinie (1.1.2.1.1.3). Für OSiP-Anwendungsfälle, die in diesen Bereich fallen, sind die Datenschutzregelungen im Wesentlichen in Teil 3 des BDSG enthalten. Für die übrigen OSiP-Anwendungsfälle hat Teil 3 keine Gültigkeit.

1.1.2.2.1.4. Datenschutzpflichten nach Teil 3 Kapitel 4 (Strafverfolgung/-vollzug)

Einzelne OSiP-Anwendungsfälle aus dem Bereich Strafverfolgung/-vollzug fallen unter Teil 3 (siehe 1.1.2.1.1.3. und 1.1.2.2.1.3.). Somit muss OSiP jedenfalls für diese Anwendungsfälle die Anforderungen von Teil 3 BDSG erfüllen. Das ist insofern für die Konzeption von OSiP relevant,

---

[30] BT-Drs. 18/11325, S. 126.

[31] Däubler, SÜG § 36 Rn. 4.

als dass Teil 3 Kapitel 4 BDSG die Anforderungen an die Datenschutzorganisation und die Datensicherheit zum Teil deutlich konkreter formuliert als die DSGVO. Diese Anforderungen finden sich im Kapitel 4 „Pflichten der Verantwortlichen und Auftragsverarbeiter". Hervorzuheben sind in diesem Zusammenhang:

- § 64 „Anforderungen an die Datensicherheit" – diese Vorschrift setzt Art. 29 JI-Richtlinie um und enthält im Vergleich zu Art. 32 DSGVO folgende wesentliche Konkretisierungen:
    - Bezugnahme auf die Technischen Richtlinien des BSI und die Empfehlungen des BSI: Diese sind von Bundesbehörden bei der Auswahl von TOM zum Datenschutz zu berücksichtigen.
    - Katalog von 14 Kontrollzielen: § 64 Abs. 2 BDSG listet Kontrollziele auf, die Verantwortliche und Auftragsverarbeiter in ihrer Risikoanalyse berücksichtigen und mit TOM behandeln müssen. Dieser Katalog ist zum Teil aus dem alten BDSG bekannt und wurde im Zuge des Erlasses des JI-Richtlinie und der Novellierung des BDSG fortentwickelt.[32] Die – im Gesetz näher definierten – Ziele lauten:
        - Zugangskontrolle
        - Datenträgerkontrolle
        - Speicherkontrolle
        - Benutzerkontrolle
        - Zugriffskontrolle
        - Übertragungskontrolle
        - Eingabekontrolle
        - Transportkontrolle
        - Wiederherstellbarkeit
        - Zuverlässigkeit
        - Datenintegrität
        - Auftragskontrolle
        - Verfügbarkeitskontrolle
        - Trennbarkeit

[32] Vgl. Freund in Schuster/Grützmacher, 2. Aufl., Art. 32 DSGVO Rn. 89.

- § 71 „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen" – diese Vorschrift entspricht weitgehend Art. 25 DSGVO (Privacy by Design). Besonders stark betont wird aber die Pflicht zur Datensparsamkeit durch:
    - Abs. 1 Satz 3: „*Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten.*", und
    - Abs. 1 Satz 4, wonach personenbezogene Daten *„zum frühestmöglichen Zeitpunkt"* zu anonymisieren oder zu pseudonymisieren sind, soweit der Verarbeitungszweck dies zulässt.
- § 74 Verfahren bei Übermittlungen – Diese Regelung ist in der DSGVO nicht enthalten (sie beruht auf der JI-Richtlinie).[33] Sie stellt besondere Bedingungen für die Übermittlung und Bereitstellung von Daten auf (die – soweit nicht ausgeschlossen – insbesondere für die Erkenntnisstellen relevant sind):
    - Abs. 1 verlangt, die Qualität übermittelter Daten zu sicherzustellen und zu überprüfen. Nach Möglichkeit sind Informationen beizufügen, mit denen der Empfänger die Richtigkeit, Vollständigkeit, Zuverlässigkeit und Aktualität der Daten überprüfen kann (Satz 2). Dies bezieht sich nicht lediglich auf übliche Prüfsummen oder Signaturen zur Integritätsprüfung, sondern auf die inhaltliche Richtigkeit und Aktualität.[34] Die übermittelten Metadaten müssen es dem Empfänger erlauben, den Informationsgehalt der übermittelten Daten einzuordnen. – Eine Anwendung wie OSiP muss diese Anforderungen etwa bei der Gestaltung von Datenformaten berücksichtigen, die für die auszutauschenden Daten vorgesehen sind.
    - Abs. 2: Gelten für die Daten besondere Verarbeitungsbedingungen, müssen sie mit einem entsprechenden Hinweis versehen oder markiert werden. Auch dies sollte IT-seitig ggf. durch entsprechende Datenfelder oder Metadaten ermöglicht werden. Welche konkreten Kennzeichnungen vorzunehmen sind, ergibt

[33] Vgl. Schwichtenberg in Kühling/Buchner, 4. Aufl., § 74 BDSG Rn. 1.

[34] Vgl. Schwichtenberg in Kühling/Buchner, 4. Aufl., § 74 BDSG Rn. 2b.

sich aus dem jeweils anzuwendenden Fachrecht und ist von den Verantwortlichen vorzugeben.

- § 76 Protokollierung – die Frage der Protokollierung ist in der DSGVO nicht ausdrücklich geregelt, was in der Praxis zu erheblichen Unklarheiten hinsichtlich der Protokollierungspflicht führt. Zwar ist allgemein anerkannt, dass sich eine gewisse Pflicht zur Protokollierung von Aktionen, mit denen personenbezogene Daten in IT-Systemen eingegeben oder sonst verarbeitet werden, zwingend aus Art. 25, 32 DSGVO (bzw. für die JI-Richtlinie: Art. 19 und Art. 29) und insbesondere der *Rechenschaftspflicht* (Art. 5 Abs. 2 DSGVO; Art. 4 Abs. 4 JI-Richtlinie) ergeben muss. Da mit den Protokolldaten jedoch häufig wiederum personenbezogene Daten erzeugt werden, ist höchst unklar, was genau in welchem Umfang wie lange zu protokollieren ist. Hier liefert § 76 BDSG (basierend auf Art. 25 JI-Richtlinie) im Gegensatz zur DSGVO eine sehr hilfreiche Konkretisierung, insbesondere hinsichtlich:
    - Umfang der Protokolle: Verantwortliche und Auftragsverarbeiter müssen mindestens die in Abs. 1 genannten Vorgänge protokollieren. Bei Abfragen und Offenlegungen muss das Protokoll die in Abs. 2 genannten Informationen umfassen.
    - Speicherfrist (Abs. 4): Löschung am Ende des auf die Generierung folgenden Jahres.
- § 62 „Auftragsverarbeitung" – diese Vorschrift beruht auf Art. 22 JI-Richtlinie und ist teils spezifischer als Art. 28 DSGVO, insbesondere durch Bezugnahme auf die eben bereits genannten Datensicherheits-Pflichten:
    - Der Auftragsverarbeiter ist darauf zu verpflichten, alle nach § 64 BDSG erforderlichen Maßnahmen zu ergreifen.
    - Der Auftragsverarbeiter ist darauf zu verpflichten, dem Verantwortlichen die Protokolle zur Verfügung zu stellen (z.B. über die Anwendung selbst), § 62 Abs. 5 Satz 5 DSGVO).

1.1.2.2.2. Spezialgesetzliche Regelungen

Das dem jeweiligen Anwendungsfall zugrunde liegende Fachrecht enthält neben der Rechtsgrundlage für die Datenverarbeitung der zuständigen Stelle, der mitwirkenden Stellen und der Erkenntnisstellen zum Teil auch weitergehende datenschutzrechtliche Regelungen, die dem

BDSG – soweit anwendbar – vorgehen. Das Zielbild von OSiP muss im Rahmen einer Anforderungserfassung gegen die im Fachrecht formulierten Anforderungen abgeglichen werden.

So regeln die §§ 20-23 SÜG die Verarbeitung von Daten im Rahmen verschiedener Anwendungsfälle durch die zuständige Stelle, die mitwirkenden Stellen und die Erkenntnisstellen (soweit es sich um Bundesbehörden handelt).

Z.B. muss das Bereitstellungsmodell der Anforderung des § 21 Abs. 3 SÜG genügen, wonach die mitwirkende Behörde personenbezogene Daten nur an öffentliche Stellen übermitteln darf. Dies wirft die Frage auf, ob eine solche Regelung dem Betrieb von OSiP durch einen nicht-öffentlichen IT-Dienstleister entgegensteht. Im Ergebnis sprechen jedoch gute Gründe dafür, dass dies bei einem als Auftragsverarbeiter verpflichteten nicht-öffentlichen Dienstleister nicht der Fall ist (dieser also beauftragt werden und die Daten dann weisungsgebunden verarbeiten darf). Dies lässt sich wie folgt herleiten:

§ 21 Abs. 3 SÜG ist eine datenschutzrechtliche Norm und vor dem Lichte des europäischen und deutschen Datenschutzrechts auszulegen. Nach dessen Konzeption ist zu unterscheiden zwischen Auftragsverarbeitern[35] und Dritten[36]. Bei Auftragsverarbeitern handelt es sich im Sinne des Datenschutzrechts um Empfänger,[37] nicht aber um Dritte.[38] Der Begriff „übermitteln" bezeichnet im Sinne des Datenschutzrechts die Offenlegung an einen Dritten, nicht aber die Offenlegung an einen sonstigen Empfänger (nämlich insbesondere an einen Auftragsverarbeiter).[39] Für Auftragsverarbeiter gilt insofern eine „Privilegierung" – ihm darf der Verantwortliche Daten offenlegen, ohne dass es auf die gesetzlichen Erfordernisse der Rechtmäßigkeitsprüfung etc. ankommt.[40] – Trotz dieser Auslegung ist vor dem Hintergrund der gesetzlichen Wertung von § 21 Abs. 3 SÜG zu empfehlen, im Falle des Einsatzes eines nicht-öffentlichen IT-Dienstleisters erst Recht auf eine Ende-zu-Ende-Verschlüsselung zu setzen. Denn beim Einsatz einer Ende-zu-Ende-Verschlüsselung, die ausschließt, dass der Dienstleister mit den Daten im Klartext

---

[35] Vgl. § 46 Nr. 8 BDSG iVm § 36 Abs. 1 Nr. 2 SÜG sowie Art. 4 Nr. 8 DSGVO und Art. 3 Nr. 9 JI-RL.

[36] Vgl. § 42 Abs. 1 Nr. 1 BDSG iVm § 36 Abs. 1 Nr. 2 SÜG sowie Art. 4 Nr. 10 DSGVO.

[37] Vgl. § 46 Nr. 9 BDSG iVm § 36 Abs. 1 Nr. 2 SÜG sowie Art. 4 Nr. 9 DSGVO und Art. 3 Nr. 10 JI-RL (jeweils: *„unabhängig davon, ob es sich … um einen Dritten handelt"*).

[38] Vgl. Art. 4 Nr. 10 DSGVO.

[39] Vgl. § 42 Abs. 1 Nr. 1 BDSG iVm § 36 Abs. 1 Nr. 2 SÜG.

[40] Hartung in Kühling/Buchner, 4. Aufl., Art. 4 Nr. 10 DSGVO Rn. 8.

in Berührung kommt, ergibt sich mit Blick auf die EuGH-Rechtsprechung ein zusätzliches Argument dafür, dass insofern keine Übermittlung von personenbezogenen Daten an den Dienstleister vorliegt.[41]

1.1.2.2.3. Rechtsverordnungen und Verwaltungsvorschriften

Aspekte des Datenschutzes können auch in untergesetzlichen Vorschriften des Bundes geregelt sein.

Anforderungen an die Verarbeitung können sich etwa aus Ausführungsbestimmungen zum Fachrecht ergeben. Für OSiP-Anwendungsfälle sind insbesondere allgemeine Verwaltungsvorschriften und auf § 35 SÜG gestützte Ausführungsregelungen des Bundes (z.B. zur Einstufung und Behandlung von Verschlusssachen) zu beachten. § 35 SÜG ermächtigt das BMI zum Erlass allgemeiner Verwaltungsvorschriften zur Ausführung des SÜG. Darüber hinaus sieht § 34 SÜG eine Verordnungsermächtigung vor (u.a. zur Bestimmung zuständiger Ressorts und betroffener Einrichtungen). Entsprechende Ausführungsvorschriften erscheinen aus datenschutzrechtlicher Sicht im Zweifel nicht von grundlegender Bedeutung für die übergeordnete Konzeption von OSiP; ggf. daraus abzuleitende Anforderungen sollten auf einer nachgelagerten Stufe im Rahmen ganz konkreter Bedarfserfassungen für einzelne Anwendungsfälle erfasst und behandelt werden (etwa als fachliche Bedarfe, die über OSiP-Fachgruppen gebündelt und an das Produktteam herangetragen werden).

Da über OSiP übermittelte Erkenntnisse ggf. als VS NfD klassifiziert sind, sind jedoch insoweit die Verwaltungsvorschriften zur Ausgestaltung des materiellen Geheimschutzes bei der Gestaltung von OSiP zu beachten (1.3.).

1.1.2.3. Länder

Im Ausgangspunkt ist hier auf die Ausführungen unter 1.1.2.2 zu verweisen: Grundsätzlich wird die Datenverarbeitung durch deutsche Behörden durch die DSGVO geregelt. Soweit die DSGVO nicht anwendbar ist – insbesondere im Bereich der nationalen Sicherheit oder der JI-Richtlinie (siehe im Einzelnen 1.1.2.1.) – oder Öffnungsklauseln enthält, kann der deutsche Gesetzgeber den Datenschutz regeln. Die Länder sind dabei zuständig für das Verwaltungsverfahren der

[41] Vgl. EuGH, Urt. V. 04.09.2025 (Rs. C-413/23P), wonach pseudonymisierte Daten für eine Stelle, die keinen Zugriff auf die Zuordnungsregel hat, anonym sind. Dies ist zwanglos auf verschlüsselte Daten, für die kein Zugriff auf die Schlüssel besteht, übertragbar.

Landesbehörden und die damit verbundene Datenverarbeitung durch die Landesbehörden im Rahmen ihrer Aufgabenerfüllung. Für diese Datenverarbeitung gilt grundsätzlich das jeweilige LDSG (1.1.2.3.1).

Das dem jeweiligen OSiP-Anwendungsfall zugrunde liegende Fachrecht enthält jedoch grundsätzlich die datenschutzrechtliche Rechtsgrundlage für die Verarbeitung und zum Teil auch weitergehende datenschutzrechtliche Regelungen. Soweit es sich dabei um Landesrecht handelt – wie bei den Hafensicherheitsgesetzen – siehe (1.1.2.3.2).

Schließlich gibt es untergesetzliche Ausführungsvorschriften der Länder zu den OSiP-Anwendungsfällen, die zum Teil auch den Datenschutz betreffen (1.1.2.3.3).

1.1.2.3.1. LDSG

Soweit die Landesbehörden handeln, ist grundsätzlich das jeweilige Landesdatenschutzgesetz einschlägig. Dies gilt auch, wenn die Länder Bundesrecht ausführen. Damit erfasst das jeweilige LDSG die Verarbeitung personenbezogener Daten im Rahmen der OSiP-Anwendungsfälle durch Landesbehörden, soweit diese

- als zuständige Behörde eine ZSÜ durchführen (unabhängig davon, ob die Prüfung auf Landesrecht oder Bundesrecht beruht), oder
- als Erkenntnisstelle oder sonst an dem Verfahren beteiligt sind.

In diesen Fällen ist – soweit nicht die DSGVO den Sachverhalt abschließend regelt – grundsätzlich das Landesdatenschutzgesetz anwendbar.[42]

1.1.2.3.2. Spezialgesetzliche Regelungen

Zu beachten ist auch hier, dass die für den OSiP-Anwendungsfall geltenden Rechtsgrundlagen zum Teil Spezialregelungen zum Datenschutz enthalten und zum Teil die Geltung des jeweiligen LDSG ausdrücklich einschränken. Zum Teil wird die Datenverarbeitung detailliert geregelt. Ein Beispiel sind die Regelungen über die Datenverarbeitung in den Hafengesetzen der Länder.

---

[42] Vgl. etwa Art. 1 Abs. 1 Satz 1 BayDSG (Geltung für Behörden und sonstige öffentliche Stellen Bayerns); § 2 Abs. 1 BlnDSG (Geltungsbereich für öffentliche Stellen des Landes Berlin); § 1 Abs. 1 HDSIG (Geltung für öffentliche Stellen des Landes Hessen); § 5 Abs. 1 DSG NRW (Anwendungsbereich des DSG NRW).

1.1.2.3.3. Rechtsverordnungen und Verwaltungsvorschriften

Aspekte des Datenschutzes können auch in untergesetzlichen Vorschriften der Länder geregelt sein.

Anforderungen an die Verarbeitung können sich etwa aus Ausführungsbestimmungen zum Fachrecht ergeben. So konkretisieren auf Landesebene je nach Anwendungsfall zum Teil Rechtsverordnungen die Durchführung von Sicherheits- und Zuverlässigkeitsprüfungen (und ggf. die Datenverarbeitung). Beispielsweise enthalten die Landes-SÜGs Ermächtigungen zum Erlass von Verwaltungsvorschriften zur Regelung des Verfahrens;[43] entsprechend Vorschriften gelten aber jeweils nur, soweit das jeweilige Landes-SÜG die Rechtsgrundlage für die ZSÜ ist. Diese Ermächtigungen sind im Allgemeinen durch Erlass entsprechender Vorschriften ausgeübt worden.[44]

Entsprechende Ausführungsvorschriften erscheinen aus datenschutzrechtlicher Sicht im Zweifel nicht von grundlegender Bedeutung für die übergeordnete Konzeption von OSiP; ggf. daraus abzuleitende Anforderungen sollten auf einer nachgelagerten Stufe im Rahmen ganz konkreter Bedarfserfassungen für einzelne Anwendungsfälle erfasst und behandelt werden (etwa als fachliche Bedarfe, die über OSiP-Fachgruppen gebündelt und an das Produktteam herangetragen werden).

Konkret zu OSiP (in der aktuellen Form) gibt es Verwaltungsvorschriften in NRW. Zum einen verweisen dort Facherlasse (z.B. zum Staatsangehörigkeitsrecht) punktuell auf OSiP als Übermittlungsweg.[45] Außerdem liegt ein Gemeinsamer Runderlass von sieben Ministerien zu OSiP vor, der die Auftragsverarbeitung anordnet (OSiP-Auftragsverarbeitungsrichtlinie).[46] Diese Ver-

---

[43] Vgl. etwa § 34 BremSÜG, § 31 SÜG RP, § 35 SächsSÜG und § 33 HmbSÜGG.

[44] Vgl. für Bayern: Allgemeine Verwaltungsvorschrift zur Ausführung des BaySÜG (VVBaySÜG), BayMBl. 2020 Nr. 484; für Sachsen: VwV des Sächsischen Innenministeriums zur Ausführung des SächsSÜG (VwVSächsSÜG); für Schleswig-Holstein: Allg. VwV zum LSÜG; für Niedersachsen: Allg. VwV zur Ausführung des Nds. SÜG; für NRW: VwV gem. § 33 SÜG NRW (Runderlass IM NRW v. 27.05.1998; zusätzlich: neue VSA NRW 18.06.2024; für das Saarland: Allgemeine Verwaltungsvorschrift zum Saarländischen SÜG (AV SSÜG, Amtsbl. I 17.02.2022).

[45] Ausführungserlass zum Staatsangehörigkeitsrecht, Runderlass des MKJFGFI vom 11. November 2022 (511-26.13.00-2020-0000675 5), Ziffer 1.3.1.2.

[46] Gemeinsamer Runderlass, OSiP-Auftragsverarbeitungsrichtlinie, vom 15. August 2024, MBl. NRW 2024 (32), S. 963-980.

waltungsvorschrift regelt die Verarbeitung personenbezogener Daten im Rahmen der ZSÜ unter Nutzung von OSiP als Verfahrensweg und gilt für sämtliche OSiP-Anwendungsfälle, die in den Zuständigkeitsbereichen der beteiligten Ministerien durchgeführt werden.

- Die OSiP-Auftragsverarbeitungsrichtlinie (NRW) soll vor allem Rechtssicherheit im Hinblick auf die DSGVO schaffen, indem sie festlegt, dass die jeweils fachlich zuständige Behörde (z.B. die Waffenbehörde) der datenschutzrechtliche Verantwortliche ist, während der Landesbetriebs Information und Technik NRW (IT.NRW) als Auftragsverarbeiter fungiert. Aus hiesiger Sicht handelt es sich dabei um eine Klarstellung (also nicht um einen erforderlichen Rechtsakt), da auch ohne dies nach geltendem Recht (mangels konkreter Rechtsgrundlage für einen OSiP-Betreiber zur eigenverantwortlichen Verarbeitung von Daten im Rahmen des IT-Betriebs) die Auftragsverarbeitung die einzig rechtlich tragfähige Gestaltungsform für den OSiP-Betrieb ist. Die Auftragsverarbeitung könnte aber auch etwa durch Abschluss eines Vertrags – z.B. als Teil von Produktnutzungsbedingungen von OSiP – wirksam vereinbart werden.
- Ferner wird eine Nutzungspflicht statuiert, wonach die zuständigen Stellen die Erkenntnisstellen über OSiP beteiligen müssen. Damit wird ein hoher Grad an Verbindlichkeit des Verfahrens und ein einheitlicher Standard im Land NRW erreicht.

1.1.2.4. Zwischenergebnis und Folgerungen für TOM-Schutzziele

Die Ausführungen unter 1.1.2.1 bis 1.1.2.3 zeigen, dass der datenschutzrechtliche Rahmen bei einem länderübergreifenden Projekt wie OSiP mit verschiedenen beteiligten Stellen und diversen Anwendungsfällen im Detail komplex ist. Dies ergibt sich aus der föderalen Struktur und den beiden zu beachtenden Datenschutzregimen des Unionsrechts (DSGVO und JI-Richtlinie). Gleichwohl gilt, dass das auf die verschiedenen OSiP-Beteiligten anwendbare Datenschutzrecht ganz wesentlich durch vereinheitlichte (DSGVO) bzw. harmonisierte (JI-Richtlinie) Prinzipien bestimmt ist. Dies erlaubt in der Konzeptionierungsphase gewisse vereinfachende Annahmen.

Ein konkretes Beispiel sind die zu beachtenden TOM-Schutzziele. Die DSGVO gibt diese in sehr allgemeiner Form in Art. 32 DSGVO vor, die JI-Richtlinie in Art. 29 JI-Richtlinie, der (für den Bund) in § 64 BDSG umgesetzt ist. Für die technische Konzeptionierung genügt es, sich an den TOM-Schutzzielen zu orientieren, dies sich aus eben diesen Normen ergeben. Diese Schutzziele sind umfassend und die Vereinheitlichung/Harmonisierung durch das EU-Recht rechtfertigen die Annahme, dass die Landesdatenschutzgesetze keine wesentlichen zusätzlichen Schutzziele vorgeben. Dies lässt sich wie folgt begründen:

- Für den Bereich der DSGVO ist mangels expliziter Öffnungsklausel zu Art. 32 DSGVO bereits umstritten, ob die Mitgliedstaaten überhaupt eigene Regelungen im Bereich des Art. 32 DSGVO erlassen und damit eigene Schutzziele vorgeben dürften.[47] Tatsächlich enthalten die LDSG zum Teil Regelungen, die aber im Wesentlichen den Art. 32 DSGVO ganz oder teilweise wiederholen (siehe etwa § 3 LDSG BW).
- Für den Bereich der JI-Richtlinie geht die Regelung des § 64 BDSG – mit ihren 14 Schutzzielen – bereits über den Art. 29 JI-Richtlinie hinaus (der genau besehen 11 Schutzziele enthält; die letzten beiden sind unter einem Buchstaben zusammenfasst). Hier, also im Bereich der JI-Richtlinie, gibt es zwar theoretisch Spielraum für die Länder, weitere Schutzziele vorzugeben. Der Art. 29 JI-Richtlinie bildet aber die zwingende Vorgabe und der § 64 BDSG mit seinen drei weiteren Schutzzielen in der Praxis die Orientierung. Einzelne von den Ländern hinzugefügte Schutzziele (z.B. § 78 Abs. 2 Nr. 15 PolG BW: „Organisationskontrolle")[48] haben im Zweifel keine zusätzlichen Folgen für die Konzipierung von OSiP.

Das Vorstehende gilt für die Konzeptionierung. Im Einzelfall bestehende spezialgesetzliche Anforderungen müssten in späteren Phasen von den nutzenden öffentlichen Stellen gemeldet und geprüft werden.

1.2. IT-Sicherheit

Im EU-Recht gibt es neben der DSGVO (die insbesondere in Art. 32 DSGVO Regelungen zum technisch-organisatorischen Datenschutz enthält) eine Reihe von Regelungen zur IT-Sicherheit, die für OSiP relevant sind. Hervorzuheben sind dabei die neuen Vorschriften zur IT-Sicherheit kritischer Infrastrukturen. Dabei ist zu beachten, dass EU-Verordnungen unmittelbar gelten, während EU-Richtlinien nur mittelbare Vorgaben enthalten, die in deutsches Recht zu transformieren sind (1.2.1.).

---

[47] Für einen „impliziten Spielraum" aufgrund der rudimentären Vorgaben des Art. 32 DSGVO Roßnagel, DuD 2017, 277, 279; ihm folgend Keber in Debus/Sicko, LDSG BW, § 3 Rn. 2.

[48] § 78 Abs. 2 Nr. 15 PolG BW: *„Im Fall einer automatisierten Verarbeitung hat die Polizei nach einer Risikobewertung folgende Maßnahmen zu ergreifen: Gestaltung der innerbehördlichen Organisation in einer Weise, die den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).*"

Im Rahmen der Bund/Länder-Zusammenarbeit im Bereich der Informationstechnik auf Grundlage von Art. 91c GG und des IT-Staatsvertrags (IT-StV) sind – durch Beschlüsse des IT-Planungsrats – weitere zentrale Normen zur IT-Sicherheit erlassen worden. Zentrale Vorgaben für die OSiP-Architektur ergeben sich aus der Leitlinie Informationssicherheit und der Föderalen IT-Architekturrichtlinie (1.2.2).

Auf Bundesebene ergeben sich Anforderungen an die IT-Sicherheit aus dem BSIG (welches demnächst im Zuge der NIS2-Umsetzung novelliert wird), dem IT-NetzG, dem OZG (das allerdings nur auf einen Randbereich von OSiP anwendbar ist), dem SÜG (Geheimschutz für VS-NfD) und relevanten Verwaltungsvorschriften (1.2.3.).

Die Länder haben eine Vielzahl von Regelungen im Bereich der IT-Sicherheit der Verwaltung getroffen (1.2.4.).

1.2.1. EU

Die EU hat im Bereich der Informationssicherheit (inkl. Datensicherheit; IT-Sicherheit) insbesondere folgende Rechtsakte erlassen:

Rechtsakt	Unmittelbare rechtliche Geltung	Relevanz für OSiP
Cybersecurity Strategy 2013 JOIN(2013) 1	**Nein**	Nicht direkt. Nur Rahmen für die IT-Sicherheitsgesetzgebung.
Datenschutz-Grundverordnung (DSGVO) VO (EU) 2016/679	**Ja** (Verordnung) Zur Anwendbarkeit im Einzelnen siehe 1.1.2.1).	Grundlegende Vorgaben zur Sicherheit der Datenverarbeitung (s. 1.1.1.3), insbesondere: Art. 25 (Privacy by Design) Art. 32 (TOM) Art. 28 Abs. 1, 3 (Auswahl und Verpflichtung von Auftragsverarbeitern)
Cybersecurity Act (CSA) VO (EU) 2019/881	**Ja** (Verordnung)	Indirekt: Der CSA ist die Rechtsgrundlage der ENISA als Cybersicherheitsbehörde der EU. Außerdem schafft er einen Rechtsrahmen für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten.
Network and Information Security Directive (NIS2-RL) RL (EU) 2022/2555	**Nein** (Richtlinie) Umsetzung durch NIS2UmsG mit Änderung des BSIG steht bevor.	Die RL verschärft die Anforderungen im KRITIS-Bereich, die in Deutschland u.a. durch Änderung des BSIG umgesetzt werden. Die Regelungen des BSIG-E werden voraussichtlich auf den IT-Dienstleister anwendbar sein (II.4.2.2.3.2).

NIS2-UmsVO Durchführungsverordnung nach Art. 21 Absatz 5 NIS2-RL C(2024) 7151 (und zukünftige)	**Ja** (Verordnung) Verbindlichkeit im Zusammenspiel mit dem NIS2UmsG	In Verbindung mit der NIS2-Umsetzung im BSIG-E ist die Verordnung voraussichtlich auf den IT-Dienstleister (RZ-Betreiber) anwendbar. In jedem Fall sind die geforderten Sicherheitsmaßnahmen eine Orientierung für alle Betreiber von sensibler IT-Systeme.
Critical Entities Resilience Directive (CER-RL) RL (EU) 2022/2557	**Nein** (Richtlinie) Umsetzung durch das KRITIS-DachG.	Die CER-RL regelt die *physische* Sicherheit kritischer Infrastrukturen. Der Anwendungsbereich ist enger als bei NIS2. Erfasst sind Anlagen, die erheblich sind für kritische Dienstleistungen zur Versorgung der Allgemeinheit in bestimmten Sektoren. Nach dem KritisDachG-E sind auch bestimmte Einrichtungen der Bundesverwaltung erfasst. Der IT-Dienstleister von OSiP muss die Anwendung des KritisDachG auf ihn prüfen und ggf. die erforderlichen Maßnahmen umsetzen.
Cyber Resilience Act (CRA) VO (EU) 2024/2847	**Ja** (Verordnung)	Die Verordnung enthält Anforderungen an die Cybersicherheit von Software, die auf dem EU-Markt bereitgestellt wird. Diese könnten auf OSiP anwendbar sein. Ggf. greift jedoch die Ausnahme des Art. 2 Nr. 7 (nationale Sicherheit; Verarbeitung von Verschlusssachen).

1.2.2. Bund/Länder-Kooperation

Auf Bund-Länder-Ebene besteht im IT-Bereich eine durch Art. 91c GG verfassungsrechtlich fundierte und mit dem IT-Planungsrat und der FITKO institutionalisierte Zusammenarbeit (1.2.2.1). Verbindliche Vorgaben für OSiP zur IT-Sicherheit ergeben sich in erster Linie aus der Leitlinie Informationssicherheit (1.2.2.3) und der Föderalen IT-Architekturrichtlinie (1.2.2.5).

1.2.2.1. Zusammenarbeit nach Art. 91c GG und IT-Staatsvertrag

Den verfassungsrechtlichen Rahmen für die Zusammenarbeit von Bund und Ländern bildet Art. 91c GG. Dessen Absatz 2 ermöglicht es Bund und Ländern, Vereinbarungen zu treffen, auf deren Grundlage Regelungen von notwendigen Standards und Sicherheitsanforderungen für die Kommunikation zwischen ihren IT-Systemen getroffen werden können. Auf dieser Ermächtigung beruht der IT-Staatsvertrag (IT-StV), mit dem der IT-Planungsrat als Koordinierungsgremium gegründet wurde. Für OSiP sind die folgenden Aufgaben des IT-Planungsrats von zentraler Bedeutung:

- Koordination der Zusammenarbeit: Der IT-PLR koordiniert die föderale Zusammenarbeit in allen Fragen der Informationstechnik.
- Beschlussfassung über Standards: Der IT-PLR *beschließt* fachunabhängig und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards. Dieses explizit formulierte Recht zur Beschlussfassung ist der Kern seines Mandats im Hinblick auf technische Architekturen. Siehe dazu sogleich 1.2.2.2.
- Steuerung von Projekten und Produkten: Der IT-PLR steuert föderale IT-Projekte und -Produkte, die für die Verwaltungsdigitalisierung von Bedeutung sind.

1.2.2.2. Beschlüsse des IT-Planungsrats

Da der Gegenstand des IT-StV auch die Kompetenzen der Landesparlamente betrifft (vgl. Art. 91c Abs. 2 GG), haben die Länder jeweils Zustimmungsgesetze erlassen, die dem IT-StV innerhalb des Landes Gesetzeskraft verleihen. § 1 Abs. 7 und § 2 Abs. 2 IT-StV sehen (auf Grundlage von Art. 91a Abs. 2 GG) eine Beschlussfassung mit qualifizierter Mehrheit vor. Beschlüsse über Standards und Sicherheitsanforderungen sind verbindlich für die Verwaltungen des Bundes und der Länder (§ 2 Abs. 2 Satz 2 IT-StV). Darüber hinaus gibt es in den E-Government-Gesetzen der Länder Regelungen, die den Standardisierungs-Beschlüssen des IT-Planungsrats für IT-Interoperabilitäts- und IT-Sicherheitsstandards im jeweiligen Land Gesetzeskraft verleihen.[49]

Das Beschlussverfahren des IT-Planungsrats wird durch die Geschäftsordnung konkretisiert. Insbesondere regelt § 7 GO IT-PLR die Arten von Beschlussgegenständen (verbindliche Beschlüsse, Kenntnisnahmen u. a.) sowie das Verfahren der Beschlussfassung.

Von verbindlichen Beschlüssen über Standards und Sicherheitsanforderungen zu unterscheiden sind informatorische Kenntnisnahmen. Dies sind Tagesordnungspunkte, die als „Information" oder „Zur-Kenntnis-Nehmen" klassifiziert werden. Hierbei handelt es sich um Berichte, Sachstandsmitteilungen, Standardisierungsbemühungen anderer Stellen oder um Diskussionen, die nicht in eine formale, rechtlich bindende Entscheidung münden. Obwohl sie keine unmittelbare rechtliche Verpflichtung auslösen, sind sie von hoher strategischer Relevanz. Sie signalisieren die politische Richtung, künftige Schwerpunkte und potenzielle zukünftige Beschlussfassungen, die bei der strategischen Ausrichtung eines neuen IT-Verfahrens berücksichtigt werden sollten.

---

[49] Vgl. § 17 Satz 1 EGovG BW.

Für Produkte des IT-Planungsrats ist zudem das vom IT-PLR beschlossene Produktmanagement-Modell von Bedeutung. Die Beteiligung eines Landes an einem Produkt erfolgt regelmäßig über eine standardisierte Erklärung, mit der das Land die vorgegebenen Teilnahme- und Nutzungsbedingungen akzeptiert. Diese Annahmeerklärung konkretisiert – ergänzend zur gesetzlichen Bindungswirkung des IT-Staatsvertrags und der Beschlüsse des IT-Planungsrats – die Rechte und Pflichten der beteiligten Verwaltungen bei Nutzung und Betrieb des jeweiligen Produkts.

Für OSiP sind verschiedene konkrete Beschlüsse des IT-PLR über die IT-Sicherheit und den Datenaustausch zwischen Behörden relevant. Hervorzuheben sind die nachfolgend genannten Leitlinien und Richtlinien, die vom IT-PLR verbindlich beschlossen worden sind.

1.2.2.3. Leitlinie Informationssicherheit (IT-PLR)

Auf der eben genannten Grundlage ist die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ von 2018 (Leitlinie Informationssicherheit (IT-PLR)) vom IT-Planungsrat beschlossen worden. Diese Leitlinie bildet auf Bund-Länder-Ebene das Pendant zum UP-Bund auf Bundesebene.[50] Durch die Verabschiedung durch den IT-Planungsrat ist sie verbindlich für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder. Für Kommunen gilt die Leitlinie jedoch nur als Empfehlung.[51] Die Leitlinie formuliert Mindestanforderungen, die sich am IT-Grundschutz des BSI, dem IT-Grundschutz-Kompendium und der ISO 2700x-Normreihe orientieren.[52] Die Anforderungen betreffen folgende Handlungsfelder:

- Informationssicherheitsmanagement
- Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung
- Einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren
- Gemeinsame Abwehr von IT-Angriffen
- IT-Notfallmanagement

[50] Bostelmann in Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024.

[51] Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 2.

[52] Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 5.

Bei der Auftragsvergabe an Dritte, die Leistungen für die öffentliche Verwaltung erbringen, sind diese auf die verbindlichen Vorgaben der Leitlinie zu verpflichten.[53]

1.2.2.4. Nationale IT-Architekturrichtlinie

Die Nationale IT-Architekturrichtlinie[54] ist ein vom Föderalen IT-Architekturboard (FIT-AB) entwickeltes Rahmenwerk, das zur Nachnutzung bei der Neuentwicklung und Fortschreibung von Architekturvorgaben in der öffentlichen Verwaltung empfohlen wird. Sie wurde in der Version 1.0.0 im Beschluss 2025/17 gemeinsam mit der Föderalen IT-Architekturrichtlinie vom IT-Planungsrat beschlossen und ist daher für alle Verwaltungen von Bund und Ländern rechtlich verbindlich.

1.2.2.5. Föderale IT-Architekturrichtlinie

Mit Beschluss 2025/17 hat der IT-Planungsrat die Version 1.9.0 der Föderalen IT-Architekturrichtlinie[55] beschlossen. Sie übernimmt weitestgehend die Nationale IT-Architekturrichtlinie und fügt einzelne „föderale Ergänzungen" hinzu. Sie ist bei Planung, Errichtung und Betrieb der IT-Systeme anzuwenden, die für das Zusammenwirken von Bund und Ländern für ihre Aufgabenerfüllung benötigt werden. Somit ist sie unmittelbar relevant für die Architektur von OSiP.

Zu den von der Nationalen IT-Architekturrichtlinie und der Föderalen IT-Architekturrichtlinie formulierten „Strategischen Zielen" gehören:

- Informationssicherheit und Datenschutz (Nr. 4)
- Digitale Souveränität (Nr. 11, föderale Ergänzung)

Außerdem werden aus den Zielen „allgemeine Vorgaben" (AVn) abgeleitet. Dazu gehört die AV-08 „Sicherheit und Schutz". Nach dieser Vorgabe müssen Informationstechnik und Digitalisierung sicher gestaltet und schützt werden. Konkret umfasst dies:[56]

---

[53] Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 5.

[54] https://gitlab.opencode.de/it-architekturrichtlinien/nationale-it-architekturrichtlinie/-/wikis/uploads/986e124c9a09208d14af15de1a668a49/nationale-it-architekturrichtlinie_1.0.1.pdf.

[55] https://www.it-planungsrat.de/fileadmin/beschluesse/2025/Beschluss_2025_17_F%C3%B6derale_IT-Architekturrichtlinie_Version_1.9.0.pdf.

[56] Siehe Föderale IT-Architekturrichtlinie, V1.9.0, AV-08, S. 23.

- Informationssicherheit: Informationssicherheit muss gemäß geltenden Vorgaben gewährleistet werden (insbesondere BSI 200-1 ISMS, BSI 200-2 Grundschutz, BSI 200-3 Risikoanalyse, BSIG, BSI Info, NATO Cyber Defence).
- Geheimschutz: Die Anforderungen des Geheimschutzes müssen erfüllt werden (insbesondere Sicherheitsüberprüfung, personeller Geheimschutz, materieller Geheimschutz/Verschlusssachen).
- Datenschutz: Die gesetzlichen Regelungen bezüglich Datenschutz müssen beachtet werden (insbesondere DSGVO, BDSG, SDM und die Landesdatenschutzgesetze).

Die IT-Architekturrichtlinie weist in diesem Zusammenhang darauf hin, dass die Referenzmaßnahmen des Standard-Datenschutzmodells (SDM) nach Möglichkeit umzusetzen sind.

1.2.2.6. IT-Interoperabilitäts- und IT-Sicherheitsstandards; Beschlüsse zu Daten- und Austauschformaten (u.a. XÖV, OSCI, XTA)

Der IT-PLR beschließt „fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards" (§ 1 Abs. 1 Nr. 2 IT-StV). Da beschlossene Standards für die öffentliche Verwaltung in Bund und Ländern verbindlich sind, sind föderale Projekte wie OSiP in erster Linie unter Nutzung solcher Standards zu entwickeln.

Eine koordinierende Funktion bei der Entwicklung und dem Betrieb von IT-Standards für den Datenaustausch in der öffentlichen Verwaltung hat die „Koordinierungsstelle für IT-Standards" (KoSIT) inne. Sie ist ein Teil der Verwaltung des Landes Bremen. Der IT-PLR hat sie u.a. mit folgenden Aufgaben betraut:[57]

- Entwicklung und Betrieb von XÖV (XML in der öffentlichen Verwaltung)
- Sicherer Transport von Daten im E-Government, insb. OSCI (Online Services Computer Interface)
- Einheitlicher Zugang zu Transportverfahren, insb. XTA (XML Transport Adapter)
- Standardisierungsagenda
- Standard zum Austausch von Akten, Vorgängen und Dokumenten

[57] Siehe IT-PLR, Beschluss vom 03.03.2011 zum Errichtungskonzept des KoSIT (https://www.xoev.de/sixcms/media.php/13/Errichtungskonzept.pdf) sowie die Aufgabenliste unter https://www.xoev.de/ueber-uns/aufgabenbereiche-4970.

Die in diesem Rahmen entwickelten IT-Standards beschränken sich nicht auf fachunabhängige und fachübergreifende Standards. Zwar sind für fachspezifische Standards eigentlich die Fachministerkonferenzen zuständig. Jedoch beruft sich der IT-PLR insofern auf seine Aufgabe, die Zusammenarbeit von Bund und Ländern in Fragen der IT zu koordinieren (§ 1 Abs. 1 Nr. 1 IT-StV). Zur Gewährleistung der Interoperabilität werden daher auch Aufgaben mit Bezug zu fachspezifischen Standards von der KoSIT bzw. dem IT-PLR ausgeführt. Beispiele sind die Kompatibilität von Standards wie XMeld und XWaffe mit dem Standard XÖV.[58] In jedem Fall sind die vom IT-Planungsrat entwickeln Standards leitend für die Entwicklung darauf aufbauender fachspezifischer Standards der für OSiP relevanten Erkenntnisstellen.

1.2.2.7. Beschlüsse zum Verbindungsnetz

Das Verbindungsnetz von Bund und Ländern ist auf Grundlage von Art. 91c Abs. 4 GG und dem IT-NetzG eingerichtet worden. Das IT-NetzG schreibt vor, dass der Datenaustausch zwischen öffentlichen Stellen über dieses abgesicherte Netz erfolgen soll (siehe 1.2.3.2). Die Koordinierung der Anforderungen and das Verbindungsnetz und der Anschlussbedingungen ist dem IT-Planungsrat übertragen. Der IT-PLR hat zunächst die Beschlüsse des Vorgängergremiums betreffend das Verbindungsnetz übernommen.[59] Die Neubeauftragung des Verbindungsnetzes und dessen fortlaufender Betrieb wurden in späteren Sitzungen begleitet.[60] Insgesamt stellen diese Beschlüsse sicher, dass ein zentrales, geschütztes Netz für ebenenübergreifende IT-Verfahren zu Verfügung steht (und Regeln die Teilnahme- und Anschlussbedingungen). Ein Verfahren wie OSiP kann – und muss – unter Beachtung dieser Beschlüsse im Verbindungsnetz realisiert werden, was hohen Schutz für die übertragenen Daten bietet.

1.2.2.8. Beschluss zur Neukonzeption von OSiP

Bei der Neukonzeption von OSiP sind nicht zuletzt die auftraggebenden Beschlüsse des IT-PLR zu beachten (Beschluss 2024/52[61] und Beschluss 2025/20[62]). Der Beschluss 2025/20 legt maßgebliche Architekturziele fest:

---

[58] Vgl. IT-PLR, Errichtungskonzept KoSIT, Ziffer 2.2.

[59] Vgl. schon IT-PLR, Beschluss 2011/03 (4. Sitzung) vom 03.03.2011.

[60] Vgl. IT-PLR, Beschluss 2015/28 (18. Sitzung) vom 01.10.2015.

[61] IT-PLR, Beschluss 2024/52 (45. Sitzung) vom 13.11.2024.

[62] IT-PLR, Beschluss 2025/20 (46. Sitzung) vom 26.03.2025.

- eine medienbruchfreie und Ende-zu-Ende-verschlüsselte Lösung, die die Prinzipien Secure- und Data-Protection-by-Design berücksichtigt und einen Zero-Trust-Ansatz verfolgt,
- die Komplexität des Betriebs zu reduzieren,
- Robustheit, Effizienz und Skalierbarkeit zu steigern,
- die Homogenisierung von Schnittstellen für die unmittelbare Anbindung, Authentifizierung und Adressierung von Fachverfahren und Behördensystemen.

Diese Vorgaben, insbesondere die Reduktion der Komplexität und die Homogenisierung von Schnittstellen, legen nahe, dass ein zentralisiertes Transport- und Betriebsmodell für OSiP bevorzugt wird.

Diese sind zunächst nur Planungsziele. Sie stehen somit nicht im Rang von Standardisierungsbeschlüssen. Im Falle eines zukünftigen Beschlusses des IT-PLR über eine entsprechende, fertige Planung würden die Vorgaben jedoch mit einer Verbindlichkeit für das Verfahren OSiP ausgestattet.

1.2.3. Bund

Auf Bundesebene ergeben sich Anforderungen an die IT-Sicherheit aus dem – im Zuge der NIS2-Umsetzung demnächst novellierten – BSIG (1.2.3.1.), dem IT-NetzG (1.2.3.2.), aus dem – nur auf Teile von OSiP anwendbaren – OZG (1.2.3.3.), hinsichtlich des Geheimschutzes aus dem SÜG (1.3.1.) sowie aus relevanten Verwaltungsvorschriften (1.2.3.4.).

1.2.3.1. BSIG

Durch das BSI-Gesetz (BSIG) ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale deutsche IT-Sicherheitsbehörde mit weitreichenden Aufgaben und Befugnissen eingerichtet worden. Das Gesetz wird mit der Umsetzung der NIS2-RL demnächst neu gefasst werden. Wie schon bisher ergeben sich daraus besondere Anforderungen für die IT-Sicherheit der Einrichtungen des Bundes, insbesondere die Pflicht zur Einhaltung der Vorgaben des BSI (1.2.3.1.1.). Ferner werden im BSIG die Anforderungen an den Schutz kritischer Infrastrukturen umgesetzt, die voraussichtlich auch den zentralen IT-Dienstleister von OSiP als „(besonders) wichtige Einrichtung“ erfassen und zu einem besonderen Risikomanagement verpflichten werden (1.2.3.1.2.).

1.2.3.1.1. Vorgaben des BSI für die IT des Bundes

Der derzeit noch geltende § 8 BSIG enthält die Befugnis des BSI zur Festlegung von Mindeststandards für die IT des Bundes.[63] Diese sind für die Stellen des Bundes verbindlich.[64] Im Gegensatz zum BSI-Grundschutz, der sich nicht nur an die Verwaltung, sondern auch an Unternehmen und andere Institutionen richtet, gelten die Mindeststandards speziell für die Bundesverwaltung.[65] Für die FITKO und die Länder entfalten sie nur dann unmittelbare Bindungswirkung, wenn sie durch Beschlüsse des IT-Planungsrats oder durch landesrechtliche Regelungen übernommen werden. Für die Ausgestaltung von OSiP sind sie gleichwohl als Referenzrahmen bedeutsam, da Bundesbehörden das System nur nutzen können, wenn es ihnen die Einhaltung der einschlägigen Mindeststandards ermöglicht.

Derzeit sind auf der Website die folgenden Mindeststandards veröffentlicht:[66]

- Nutzung ressortübergreifender Kommunikationsnetze („Nutzerpflichten NdB“)
- ISMS in der IT-Konsolidierung
- Protokollierung und Detektion von Cyber-Angriffen
- Mindeststandard für Webbrowser
- HV-Benchmark
- Transport Layer Security (TLS)
- Externe Cloud-Dienste
- Mobile Device Management
- Videokonferenzdienste
- (früher) Schnittstellenkontrollen (Mindeststandard mit Wirkung zum 30.04.2024 aufgehoben, die zugrunde liegenden Anforderungen werden inzwischen über IT-Grundschutz-Bausteine und weitere BSI-spezifische Vorgaben abgedeckt).

---

[63] Vgl. die entsprechende Aufgabe in § 3 Abs. 1 Satz 2 Nr. 10 BSIG.

[64] § 8 Abs. 1 Satz 1 Nr. 1 BSIG.

[65] Brandenburg in Kipker/Reusch/Ritter, § 8 BSIG Rn. 3.

[66] Siehe www.bsi.bund.de/mindeststandards.

Im neuen BSIG wird die Befugnis zum Erlass von Mindeststandards voraussichtlich geregelt in § 44 BSIG-E. Sie wird inhaltlich teils modifiziert.[67] Nach § 44 Abs. 2 BSIG-E müssen das Bundeskanzleramt und die Bundesministerien zukünftig als zusätzliche Mindestanforderungen

- die BSI-Standards und
- das IT-Grundschutz-Kompendium

in der jeweils geltenden Fassung einhalten.

1.2.3.1.2. Anforderungen an Betreiber Kritischer Infrastrukturen

Derzeit bildet noch § 8a BSIG, der die NIS-RL der EU umsetzt, die Generalklausel für die Absicherung Kritischer Infrastrukturen. Mit der bevorstehenden Umsetzung des NIS2-RL werden die Pflichten von KRITIS-Betreibern in § 30 ff. BSIG-E neu geregelt.[68]

Für OSiP können die KRITIS-Anforderungen relevant werden, wenn der Betreiber oder die Nutzer nach § 28 BSIG-E als besonders wichtige Einrichtungen oder wichtige Einrichtungen in den Anwendungsbereich fallen. Dies ist für den technischen Dienstleister, der OSiP bereitstellen wird, sehr wahrscheinlich, da IT-Dienstleistungen zu den regulierten Tätigkeiten zählen und der Dienstleister voraussichtlich die relevanten Schwellenwerte überschreitet (siehe II.4.3.3.1.).

1.2.3.2. IT-NetzG

Das Verbindungsnetz verbindet die Netze des Bundes mit den Verwaltungsnetzen der Länder und den Kommunalnetzen. Der Bund hat nach Art. 91c GG die Gesetzgebungskompetenz zur Regelung von Einrichtung und Betrieb des Verbindungsnetzes. Diese Kompetenz wurde mit dem IT-NetzG ausgeübt. Nach § 3 Abs. 1 Satz 1 IT-NetzG erfolgt der Datenaustausch zwischen Bund und Ländern verpflichtend über das Verbindungsnetz. Lediglich im Bereich des OZG ist nach Satz 2 ein Austausch über andere Netze möglich. Festlegungen für das IT-NetzG werden durch den IT-Planungsrat als zuständiges Koordinierungsgremium per Beschluss getroffen (§ 4 IT-NetzG).

---

[67] Vgl. Gesetzentwurf der Bundesregierung vom 25.07.2025, S. 53.

[68] Vgl. Gesetzentwurf der Bundesregierung vom 25.07.2025, S. 40 ff.

Der IT-Planungsrat verabschiedet u.a. den jeweiligen Leistungskatalog des Verbindungsnetzes.[69] Danach erfüllt das Verbindungsnetz einschließlich der Verbindungsnetz-Dienste die Anforderungen der IT-Sicherheit an den Schutzbedarf „hoch" und ist für die Übertragung von VS-NfD-eingestuften Daten nach VSA-Bund geeignet. Bei der Übertragung von VS-NfD eingestuften Daten ist von den Teilnehmern sicherzustellen, dass die gesamte Kommunikationsstrecke Ende-zu-Ende für VS-NfD geeignet ist.[70]

Zur den Anforderungen, die sich aus dem IT-NetzG für OSiP ergeben, siehe III.1.1.

1.2.3.3. Onlinezugangsgesetz (OZG)

Das OZG des Bundes regelt die Bereitstellung von Verwaltungsleistungen über Onlinedienste innerhalb der Verwaltungsportale von Bund und Ländern, die zu einem Portalverbund verknüpft sind (§ 1 Abs. 1 OZG). Die geplante Architektur des neuen OSiP fällt grundsätzlich nicht unter die vom OZG geregelten Onlinedienste,[71] da dabei nicht eine Verwaltungsleistung nach außen zugänglich gemacht, sondern verwaltungsintern technisch umgesetzt wird. Insbesondere fallen die OSiP-Transportinfrastruktur und Clients, die Fachverfahren abbilden, nicht unter das OZG.

Vom OZG erfasst sind demgegenüber nur die auf OSiP aufsetzenden Online-Dienste und Schnittstellen, über die Bürgerinnen und Bürger oder Unternehmen Anträge elektronisch einreichen (z. B. über Portale bzw. Organisationskonten). Insoweit sind neben dem OZG selbst insbesondere die auf § 5 OZG und § 6 OZG beruhenden IT-Sicherheitsvorgaben (dazu nachfolgend). Für die interne OSiP-Transportinfrastruktur ergeben sich aus dem OZG keine darüber hinausgehenden spezifischen Anforderungen an die eingesetzte Kryptographie.

Für die Entwicklung und Bereitstellung länderübergreifender Onlinedienste ist das EfA-Prinzip entwickelt worden, bei dem das Gesetz eine getrennte Verantwortlichkeit zwischen der bereitstellenden Behörde und den nutzenden Behörden vorsieht (§ 8a Abs. 4 OZG). Dies ist also zu beachten, wenn ein solcher Dienst entwickelt und zentral durch eine Behörde im Sinne dieser Vorschrift bereitgestellt werden soll.

---

[69] Siehe Leistungskatalog für das NdB-Verbindungsnetz, Version 2.9.

[70] Leistungskatalog für das NdB-Verbindungsnetz, Version 2.9, Ziffer 5.1.1.

[71] Vgl. § 2 Abs. 8 OZG.

Hinsichtlich der IT-Sicherheit Im Bereich des OZG können Bund und Länder Daten auch auf anderem Weg austauschen als über das Verbindungsnetz, soweit angemessene IT-Sicherheitsstandards eingehalten sind (§ 3 Abs. 1 Satz 2 IT-NetzG).

1.2.3.3.1. IT-Sicherheitsverordnung Portalverbund (ITSiV-PV)

Die Standards zur IT-Sicherheit im Portalverbund und für die zur Anbindung an den Portalverbund genutzten IT-Komponenten sind auf Grundlage von § 5 OZG durch das BMI per Rechtsverordnung festgelegt worden (IT-Sicherheitsverordnung Portalverbund vom 6. Januar 2022 – ITSiV-PV). Die Verordnung schreibt unter anderem vor

- dass für den Portalverbund und die IT-Systeme von Bund und Ländern, die Daten mit dem Portalverbund austauschen, Maßnahmen nach dem Stand der Technik zutreffen sind (§ 2 Abs. 1 ITSiV-PV); wobei die Einhaltung des Standes der Technik vermutet wird, wenn die in der Anlage zur ITSiV-PV genannten Technischen Richtlinien des BSI eingehalten werden;
- dass die genutzten IT-Komponenten einem ISMS unterliegen, welches die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung umsetzt (§ 2 Abs. 4 ITSiV-PV), und
- dass IT-Komponenten, die unmittelbar mit dem Internet verbunden sind oder einen hohen oder sehr hohen Schutzbedarf haben, vor Anbindung an den Portalverbund einem Penetrationstest und einem Webcheck nach den Vorgaben des BSI unterzogen werden.

1.2.3.3.2. Verordnung über Standards für den Onlinezugang zu Verwaltungsleistungen (OZSV)

Architekturvorgaben und Qualitätsanforderungen für IT-Systeme, die für den übergreifenden Zugang zu Verwaltungsleistungen von Bund und Ländern genutzt werden – also auch Onlinedienste im Sinne des OZG – sind auf Grundlage von § 6 OZG durch das Bundesministerium für Digitales und Staatsmodernisierung per Rechtsverordnung festgelegt worden (Verordnung über Standards für den Onlinezugang zu Verwaltungsleistungen vom 22. September 2025 (OZSV). Die Verordnung sieht insbesondere vor

- dass IT-Systeme, die für den übergreifenden Zugang zu den Verwaltungsleistungen von Bund und Ländern genutzt werden, nach den Vorgaben der Föderalen IT-Architekturrichtlinie (1.2.2.5) auszugestalten sind (§ 1 OZSV - Architekturvorgaben),
- dass für IT-Systeme, die für den übergreifenden Zugang zu den Verwaltungsleistungen von Bund und Ländern genutzt, neu entwickelt oder grundlegend überarbeitet werden, zur Gewährleistung der Qualität Maßnahmen nach den allgemein anerkannten Regeln der Technik zu treffen sind (§ 2 Abs. 1 OZSV - Qualitätsanforderungen).

Die Einhaltung der Qualitätsanforderungen wird vermutet, wenn die Anforderungen der DIN SPEC 66336, Ausgabe April 2025, eingehalten werden.[72] Die DIN SPEC 66336 „Qualitätsanforderungen für Onlineservices und -portale der öffentlichen Verwaltung (Servicestandard" gibt u.a. folgendes vor:

- in Ziffer 5.8 Anforderungen an die „Datenschutzfreundlichkeit" (die nicht über ohnehin bestehende Datenschutzanforderungen hinausgehen, aber in einem Datenschutzkonzept für einen Onlinedienst berücksichtigt werden müssten);
- in Ziffer 5.9 Anforderungen an die Sicherheit und Vertrauenswürdigkeit, u.a.
    - die Einhaltung der TR-03172-3 des BSI (Onlinedienste); dabei handelt es sich um Teil 3 der Normengruppe TR-03172 (Portalverbund), die darüber hinaus weitere mit einem Onlinedienst in Beziehung stehende Komponenten regelt wie das Antragsrouting (TR-03172-4);
    - Webchecks, Penetrationstests und Leistungsfähigkeit; und
- in Ziffer 5.11 Anforderungen an Betrieb und Support.

Über § 6 OZG in Verbindung mit § 2 OZSV in Verbindung mit Ziff. 5.9 DIN SPEC 66336 in Verbindung mit der TR-03172-3 ergeben sich damit für einen evtl. OSiP-Antragsdienst ganz konkrete Sicherheitsanforderungen. Zum Beispiel müssen nach Ziff. 3.6 Kommunikation der TR-03172-3, Kriterium A3.6.02 für alle Kommunikationsbeziehungen des Onlinedienstes (z.B. für die Kommunikation zum Fachverfahren oder zum Antragsrouting) die Vorgaben der BSI TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 – Kommunikationsverfahren in Anwendung" eingehalten werden.

---

[72] Siehe https://servicestandard.gov.de/din-spec-66336/.

1.2.3.4. Verwaltungsvorschriften

Zur Verwaltungsdigitalisierung gibt es organisations- und dienstanweisende Regelungen auf höchster administrativer Ebene (Kabinettsbeschlüsse). Sie werden zwar nicht als Verwaltungsvorschriften bezeichnet, haben aber denselben Rechtscharakter und sind verbindliches Binnenrecht für die Bundesverwaltung. Hervorzuheben sind für den Bereich der IT-Sicherheit allgemein der UP Bund 2017 (1.2.3.4.1), mit Blick auf die Netze die „Netzstrategie der öffentlichen Verwaltung 2030" (1.2.3.4.2) und für den Bereich des „IT-Konsolidierung Bund" (ITKB) die „Informationssicherheitsrichtlinie IT-Konsolidierung Bund 2.0" (ISR ITKB) (1.2.3.4.3).

1.2.3.4.1. Umsetzungsplan Bund 2017 (UP Bund)

Auf der Ebene der Verwaltungsvorschriften bildet für die Bundesverwaltung der Umsetzungsplan Bund (UP Bund) eine Informationssicherheitsleitlinie und damit eine verbindliche Rahmenregelung für die IT-Sicherheit. Er wurde 2017 als Regierungsbeschluss erlassen und bindet die nachgeordneten Bundesbehörden. Durch den UP Bund 2017 besteht die Pflicht zu Einführung eines ISMS und zur Einhaltung der Mindeststandards des BSI; diese wurde später auch in § 8 BSI als gesetzliche Pflicht geregelt (s. 1.2.3.1.1). Außerdem gibt der UP Bund 2017 Hinweise zur Personalentwicklung im Bereich Sicherheitsmanagement, kritischen Geschäftsprozessen, Informationssicherheitsanforderungen an Dienstleister und Dienstleistungen sowie IT-Notfallprävention und IT-Krisenreaktion.[73]

1.2.3.4.2. Netzstrategie der öffentlichen Verwaltung 2030 (IVÖV)

Der IT-Rat des Bundes ist das zentrale politisch-strategische Gremium der Bundesregierung zur Steuerung der Verwaltungsdigitalisierung in Deutschland. Er hat am 25. Februar 2019 die „Netzstrategie der öffentlichen Verwaltung 2030" (IVÖV)[74] beschlossen. Damit soll die netztechnische Basis als Integrationsplattform der gesamten öffentlichen Verwaltung fortentwickelt werden. Für den Bund stellt das in der Netzstrategie enthaltene Zielbild 2030 eine verbindliche Planung dar.

---

[73] Vgl. CIO Bund, Netzstrategie für die öffentliche Verwaltung 2023, S. 6.

[74] https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-sicherheit-und-netze/netze/netzstrategie-2030.pdf. Der IT-Planungsrat hat die Eckpunkte zur Kenntnis genommen (Entscheidung 2018/52).

1.2.3.4.3. Informationssicherheitsrichtlinie IT-Konsolidierung Bund 2.0 (ISR ITKB)

Neben dem IT-Rat ist das CIO Board ein zentrales IT-Steuerungsgremium des Bundes. Seine Beschlüsse entfalten interne Bindungswirkung für alle am Projekt „IT-Konsolidierung Bund" (ITKB) beteiligten Stellen. Hervorzuheben ist hier die „Informationssicherheitsrichtlinie IT-Konsolidierung Bund 2.0" (ISR ITKB), Version 2.00 vom 27.02.2023.[75] Ihr Geltungsbereich umfasst u.a. *„IT-Lösungen für die Bundesverwaltung, die im Rahmen der IT-Dienstekonsolidierung als Basis-, Querschnitts- oder Infrastruktur-Dienste (insbesondere in den Servicemodellen PaaS oder SaaS) zentral bereitgestellt werden"*. Damit fällt nach unserem Verständnis ein Dienstleister, den die FITKO mit der Entwicklung und dem Betrieb von OSiP beauftragt, grundsätzlich nicht unmittelbar in den formalen Geltungsbereich. Die ISR ITKB gilt jedoch dann, wenn der Dienst OSiP in die IT-Dienstekonsolidierung (DK) einbezogen und den Bundesbehörden zentral über die DK bereitgestellt wird.

Im Übrigen hat das BSI auf Grundlage der ISR ITKB einen Mindeststandard für ein ISMS erlassen, der nach § 8 Abs. 1 Satz 1 BSIG für die IT-Lösungen der Bundesverwaltung im Rahmen der ITKB verbindlich ist (siehe 1.2.3.1.1).[76]

1.2.4. Länder

In den Bundesländern bestehen eine Reihe von Leitlinien und Regelungen mir Relevanz für die IT-Sicherheit. Dabei werden unterschiedliche Ansätze verfolgt. Teils ist die IT-Sicherheit in den EGovernment- bzw. Digitalisierungsgesetzen geregelt, teils in dedizierten IT-Sicherheitsgesetzen; dazwischen gibt es Mischformen.

Die vom IT-Planungsrat im Beschlusswege verabschiedeten IT-Sicherheitsstandards sind durch Transformationsklauseln der Länder im jeweiligen Land ebenfalls mit Gesetzeskraft ausgestattet (siehe oben 1.2.2.1). Dies ermöglicht die Standardisierung und vermeidet Konflikte mit den Einzelregelungen der Länder.

---

[75] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Moderner-Staat/Informationssicherheitsrichtlinie_IT-Konsol.pdf.

[76] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_ISMS_ITKB_V1_0a.pdf.

Die Tabelle in Anlage 3 gibt einen Überblick über Regelungen zur IT-Sicherheit in den Ländern.[77]

1.3. Geheimschutz

Der materielle Geheimschutz ist in den SÜG des Bundes und der Länder geregelt und in den jeweiligen Verschlusssachenanweisungen (VSA) konkretisiert. Er ist für OSiP relevant, wenn Erkenntnisstellen ihre Erkenntnisse als VS NfD einstufen und diese über OSiP übermitteln wollen. Ferner können auch Kryptomittel, die zur Verschlüsselung genutzt werden, selbst Verschlusssachen sein (§ 4 SÜG (Bund), § 59 VSA (Bund)). In diesem Fall unterliegen die Kryptomittel dem Geheimschutz unabhängig davon, ob die verschlüsselten Informationen selbst VS sind.

In jedem Fall setzt die Klassifizierung eines Dokuments oder eines Kryptomittels als Verschlusssache – und damit das Eingreifen des materiellen Geheimschutzes – eine offizielle Einstufung durch eine zuständige Behörde voraus.

1.3.1. Bund (SÜG und VSA)

Auf Bundesebene ist der materielle Geheimschutz im SÜG (Bund) geregelt. Die Konkretisierung der Geheimhaltungsregeln ist durch die Allgemeine Verwaltungsvorschrift zum Geheimschutz (Verschlusssachenanweisung – VSA) erfolgt.

Die über OSiP zu übertragenden Erkenntnisse sind zum Teil gemäß § 4 Abs. 2 Nr. 4 SÜG als VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) eingestuft. Sie unterliegen damit besonderen Geheimhaltungsregeln, die in § 4 Abs. 4 SÜG als Generalklausel formuliert sind.

Soweit Bundesbehörden Informationstechnik zur Handhabung von VS einsetzen (VS-IT), sind die Anforderungen der VSA zu beachten. Voraussetzung für den Einsatz von VS-IT ist ein Informationssicherheitskonzept nach den BSI-Standards des IT-Grundschutzes des BSI. Hinzu kommen die im Baustein „CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)“ beschriebenen Anforderungen des Geheimschutzes.[78]

---

[77] Die Tabelle basiert wesentlich auf der Darstellung von Bostelmann in Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl., § 25 Rn. 112. Sie wurde am Lehrstuhl von Prof. Dr. Hornung erstellt und unter Mihilfe der AG InfoSic des IT-PLR aktualisiert (Stand Ende 2023).

[78] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_11_1_Geheimschutz_Edition_2023.pdf.

Auch nichtöffentliche Stellen, die Verschlusssachen (befugt) erhalten, sind zum Geheimschutz verpflichtet (§ 4 Abs. 4 Satz 2 SÜG). Hierzu erfolgt in der Praxis eine vertragliche Verpflichtung auf die Regelungen des Geheimschutzhandbuchs.

Neben dem Schutz der übermittelten Nachrichten ist für OSiP zu prüfen, ob die für die geplante Verschlüsselung eingesetzten Kryptomittel (also Produkte, zugehörige Dokumente und sonstige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen) als Verschlusssachen eingestuft sind. § 59 VSA sieht die Festlegung „nationaler Kryptomittel" durch das BSI (bzw, für den Bereich des BMV durch das BAAIMBw) und „internationaler Kryptomittel" nach entsprechenden über- und zwischenstaatlichen Normen vor. Eingestufte Kryptomittel erhalten die Warnvermerke „KRYPTO" bzw. „CRYPTO"; nicht eingestufte Kryptomittel, die sicherheitsempfindliche Funktionen ausführen, den Warnvermerk „CCI". Die Rechtsfolgen für die Verwaltung und den Schutz solcher Kryptomittel sind in der VSA geregelt (§§ 59 ff.).

1.3.2. Länder (SÜG und VSA)

Im Bereich der Länder ist der materielle Geheimschutz analog zum Bund geregelt, zumeist in den SÜG der Länder in Verbindung mit einer Verwaltungsvorschrift (Verschlusssachenweisung – VSA). Die Klassifizierung und die Anforderungen entsprechen grundsätzlich denjenigen der Bundesvorschriften. Eine Übersicht über die rechtlichen Grundlagen des materiellen Geheimschutzes enthält Anlage 3.

Die VSA der Länder sind auf einem sehr unterschiedlichen Stand. Teils sind sie sehr alt und auf die Zeit vor der Verwaltungsdigitalisierung zugeschnitten. Zum Teil sind sie nur wenige Jahre alt und berücksichtigen moderne digitalisierte Arbeitsweisen. In den letztgenannten Fällen regeln sie die Anforderungen an die elektronische Weitergabe von Verschlusssachen zumeist detailliert. Dabei wird regelmäßig wiederum auf die Vorgaben des BSI verwiesen und die von diesem für VS des betreffenden Geheimhaltungsgrades zugelassenen Verschlüsselungsverfahren und -systeme.

Eine moderne Regelung mit konkreten Anforderungen an den elektronischen Schutz/Versand von VS findet sich etwa in §§ 21, 37 und 40 VSA Thüringen, die wir zusammengefasst nachfolgend wiedergeben (siehe auch Anlage 3):

- § 21 Abs. 2 VSA: Versand von Verschlusssachen soll nach Möglichkeit nicht per Post, sondern über TK-Verbindungen nach § 40 VSA erfolgen (verschlüsselt). Zuvor sind Teilnehmerverzeichnisse zu kontrollieren. Es ist ein Protokoll zu erzeugen.

- § 21 Abs. 3: VS, die mit einem vom BSI für die jeweilige Geheimhaltungsstufe zugelassenen Kryptosystem verschlüsselt wurden, bedürfen keines weiteren Schutzes. Dies gilt nicht für die Schlüssel; diese sind getrennt einzustufen und zu schützen. Nähere Informationen sind über das Amt für Verfassungsschutz zu beziehen.
- § 37: Produkte mit IT-Sicherheitsfunktionen zur Verwendung für Verschlusssachen müssen vom BSI zugelassen sein.
- § 40: Regelung zur Übertragung per TK-Verbindung (grundsätzlich verschlüsselt gemäß Vorgaben des BSI).

2. Voraussetzungen für länderübergreifenden zentralen Dienst

Frage: „*Welche rechtlichen Voraussetzungen gelten für eine länderübergreifende Nutzung eines zentralen Dienstes?*"

Kurzantwort:

Der zentrale Betrieb von OSiP ist verfassungsrechtlich zulässig. Die rechtliche Grundlage für die länderübergreifende Kooperation bildet Art. 91c GG (Zusammenarbeit bei IT-Systemen), konkretisiert durch den IT-Staatsvertrag und die Beschlüsse des IT-Planungsrats. Voraussetzung ist, dass das Verbot der Mischverwaltung gewahrt bleibt, indem die FITKO ausschließlich technische Unterstützungsleistungen erbringt und die fachlichen Sachentscheidungen bei den zuständigen Landes- bzw. Bundesbehörden verbleiben.

Der zentrale Betrieb ist auch datenschutzrechtlich zulässig. Ausgehend davon, dass die FITKO bzw. ein zentraler Betreiber keine eigene Rechtsgrundlage für die Datenverarbeitung hat (Ausnahme: Betrieb eines ggf. geplanten Antragsdienstes nach OZG), sollte das Modell der Auftragsverarbeitung gewählt werden. Der zentrale Betrieb setzt dann voraus, dass die entsprechenden Anforderungen an die Auftragsverarbeitung beachtet werden (insbesondere streng weisungsgebundene Verarbeitung; strikte Mandantentrennung).

2.1. Verfassungsrechtlicher Rahmen

Ein zentraler Betrieb eines ebenenübergreifenden IT-Verfahrens wie OSiP berührt die verfassungsrechtlich verankerte Zuständigkeitsverteilung zwischen Bund und Ländern. Die Verwaltungsräume von Bund und Ländern sind grundsätzlich getrennt, ebenso wie die Kompetenz zur Regelung des Verwaltungsverfahrens und der IT-Nutzung (2.1.1.). Die Kompetenzverteilung des Grundgesetzes ist nicht disponibel, was die Möglichkeiten für gemeinsame Verfahren begrenzt (2.1.2.). Vor diesem Hintergrund ermöglicht Art. 91c GG eine institutionalisierte, verfassungskonforme Form der Zusammenarbeit in der IT-Nutzung (E-Government). In diesem Rahmen kann OSiP als zentrales IT-Verfahren betrieben werden. Dabei darf allerdings die Zurechenbarkeit fachlicher Sachentscheidungen zu den jeweils zuständigen Behörden nicht berührt oder aufgehoben werden.[79]

[79] Vgl. BeckOK InfoMedienR/Gersdorf/Zäper GG Art. 91c Rn. 1 ff.

2.1.1. Kompetenzordnung und Vollzug

Der Einsatz von IT durch die öffentliche Verwaltung zur Erledigung ihrer Aufgaben betrifft Fragen der Verwaltungsorganisation und des Verwaltungsverfahrens. Für die Gestaltung des IT-Einsatzes ist daher maßgeblich, welcher Verwaltungsträger (Bund oder Land) nach dem Grundgesetz befugt ist, Verwaltungsorganisation und -verfahren zu regeln. Nach den allgemeinen Kompetenzregeln der Art. 30, 70 Abs. 1 GG sind die Länder für den Vollzug von Gesetzen und die Organisation ihrer Verwaltung grundsätzlich selbst zuständig (2.1.1.1.). Nur in einzelnen Bereichen ist die Bundesverwaltung zuständig (2.1.1.2.). Die Vollzugszuständigkeit der jeweiligen Gesetze ist in der Übersicht über die maßgeblichen Rechtsgrundlagen (Anlage 1) dargestellt.

2.1.1.1. Verwaltungsvollzug durch die Länder

So führen die Länder zunächst aufgrund der ihnen in Art. 30 GG zugewiesenen allgemeinen Staatsgewalt und Organisationshoheit ihr Landesrecht durch Landesbehörden in eigener Verantwortung aus und bestimmen insoweit auch das Verwaltungsverfahren.

Zudem erfolgt auch die Ausführung von Bundesgesetzen im Regelfall als eigene Angelegenheit der Länder (Art. 83 GG). Alternativ erfolgt, sofern vom Grundgesetz vorgesehen und gesetzlich angeordnet, die Ausführung von Bundesrecht als Auftragsverwaltung (Art. 85 GG), wobei es sich ebenfalls um eine Form der Landesverwaltung handelt.[80] Die organisatorische Ausgestaltung des Vollzugs und das Verwaltungsverfahren bestimmen die Länder, soweit Bundesgesetz nichts anderes bestimmt (Art. 84 GG, Art. 85 GG).

2.1.1.2. Verwaltungsvollzug durch den Bund

Nur in einzelnen Gesetzgebungsbereichen ist schließlich die bundeseigene Verwaltung vorgesehen, also der Vollzug durch Bundesbehörden (vgl. Art. 86, 87 GG).

2.1.2. Verbot der Mischverwaltung

Jede Verwaltungsaufgabe ist in eigener Verantwortung zu erfüllen. Dieser Grundsatz wird durch das Verbot der Mischverwaltung[81] konkretisiert. Es besagt insbesondere:

---

[80] Suerbaum in BeckOK, 63. Ed., Art. 85 GG (Einl.).

[81] Vgl. Weber kompakt, Rechtswörterbuch, Mischverwaltung, 12. Edition 2025.

- der Bund darf ohne ausdrückliche verfassungs- oder einfachgesetzliche Ermächtigung keine bindenden organisatorischen oder fachlich-technischen Vorgaben für den Landesvollzug machen,
- ebenso dürfen Länder ihre Hoheitsaufgaben nur auf eine gemeinsame oder fremde Einrichtung übertragen, wenn hierfür eine Rechtsgrundlage besteht.

Ein zentraler IT-Betrieb, wie der geplante Betrieb von OSiP, muss deshalb auf eine ausdrückliche Ermächtigung zur Kooperation gestützt werden. Eine solche Ermächtigung findet sich in Art. 91c GG sowie dessen einfachrechtlicher Konkretisierung durch den IT-Staatsvertrag.[82] Art. 91c GG modifiziert das Verbot der Mischverwaltung in zulässigem Rahmen, indem er eine institutionalisierte Kooperation zur ebenenübergreifenden Nutzung von IT-Verfahren in der Verwaltung erlaubt, ohne die Zurechenbarkeit von Sachentscheidungen aufzuheben.[83]

2.1.3. Art. 91c als Kooperationsnorm

Art. 91c GG schafft einen Rahmen für die IT-Kooperation von Bund und Ländern, in dem OSiP – auch als zentraler Dienst – betrieben werden kann. Die Kooperation bleibt verfassungskonform, solange zentrale IT-Stellen keine hoheitlichen Sachentscheidungen treffen, Standards auf geeigneter Grundlage (Art. 91c GG/IT-StV) beruhen und Verantwortlichkeiten klar zugewiesen sind.

Im Einzelnen enthält Art. 91c GG folgende Regelungen:

2.1.3.1. Hintergrund und Zweck

Art. 91c GG wurde im Zuge der Föderalismusreform II im Jahr 2009[84] eingefügt und 2017 durch Abs. 5 ergänzt.[85] Die Norm bildet die verfassungsrechtliche Grundlage für die zulässige institutionelle Kooperation von Bund und Ländern in Angelegenheiten der Informationstechnik, ohne die Eigenverantwortung der Verwaltungsebenen nach Art. 30, 83 GG aufzugeben.

---

[82] BeckOK GG/Wischmeyer, Art. 91c Rn. 14, 17.

[83] Specht/Mantz, Handbuch Datenschutzrecht (2019) Rn. 89–92.

[84] Gesetz vom 29. Juli 2009 (BGBl. I S. 2248).

[85] BT-Drs. 16/12410, S. 13 f.

Die Vorschrift erlaubt ein koordiniertes, standardisiertes und sicheres Zusammenwirken der Verwaltungsebenen im IT-Bereich und stellt sicher, dass gemeinsame Strukturen nicht zu einer Kompetenzverschiebung führen.[86]

Hintergrund der Neuregelung war die Erkenntnis, dass der zunehmende Bedarf an föderal übergreifender IT-Koordination ohne ausdrückliche Verfassungsgrundlage zu einer rechtlichen Unsicherheit führen konnte. Insbesondere bestand die Gefahr, dass eine informelle oder rein vertragliche Kooperation in den Bereich der verfassungsrechtlich unzulässigen Mischverwaltung geraten könnte.[87] Art. 91c GG soll daher eine zulässige Form der institutionellen Kooperation eröffnen, die einerseits gemeinsame technische Interoperabilitäts- und Sicherheitsstandards ermöglicht, andererseits die Organisationshoheit der beteiligten Körperschaften wahrt.[88]

2.1.3.2. Systematik der Absätze 1-5

Die Vorschrift enthält folgende Kooperationsformen und Zuständigkeitsregelungen:

2.1.3.2.1. Allgemeine Zusammenarbeit (Abs. 1)

Art. 91c Abs. 1 GG erlaubt Bund und Ländern, bei Planung, Errichtung und Betrieb der für ihre Aufgabenerfüllung benötigten IT-Systeme zusammenzuwirken. Der Begriff der IT-Systeme ist weit und zukunftsoffen zu verstehen; die Norm soll dauerhafte, rechtssichere Kooperationsformen ermöglichen.[89] Die Konkretisierung erfolgt durch den IT-Staatsvertrag (IT-StV). Der IT-Planungsrat koordiniert die Zusammenarbeit, setzt fachübergreifende Standards und wird seit 1. Januar 2020 von der FITKO als „gemeinsamer Einrichtung" (iSd IT-StV) operativ unterstützt.

2.1.3.2.2. Gemeinsame Standards (Abs. 2)

Art. 91c Abs. 2 GG ermächtigt zu Vereinbarungen über Kommunikationsstandards und Sicherheitsanforderungen. Wird das qualifizierte Mehrheitsprinzip (Abs. 2 S. 2) genutzt, bedürfen solche Vereinbarungen eines Staatsvertrages mit Parlamentszustimmung – dies ist im IT-StV umgesetzt (insb. § 1 Abs. 7 IT-StV).

---

[86] BT-Drs. 16/12410, S. 8 f.

[87] Vgl. BverfGE 119, 331 („ARGEn") – zum Verbot der Mischverwaltung und zum Grundsatz eigenverantwortlicher Aufgabenwahrnehmung.

[88] BeckOK GG/Gersdorf/Zäper, Art. 91c Rn. 1–2.

[89] BeckOK InfoMedienR/Gersdorf/Zäper GG Art. 91c Rn. 4.

2.1.3.2.3. Gemeinschaftlicher Betrieb (Abs. 3)

Art. 91c Abs. 3 GG erlaubt den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung gemeinsamer Einrichtungen. Darauf lassen sich föderal genutzte Basiskomponenten stützen, sofern die fachliche Entscheidungshoheit unberührt bleibt.

2.1.3.2.4. Verbindungsnetz (Abs. 4)

Art. 91c Abs. 4 GG verleiht dem Bund die Befugnis, ein Verbindungsnetz für die gemeinsame Nutzung durch Bund und Länder zu errichten und zu betreiben. Das Verbindungsnetz dient dem sicheren, standardisierten Datenaustausch. Der Bund hat von der Befugnis durch Erlass des IT-NetzG Gebrauch gemacht (1.2.3.2). Ausgestaltung und Nutzung des Verbindungsnetzes werden durch Beschlüsse des IT-Planungsrats konkretisiert.

2.1.3.2.5. Onlinezugang zu Verwaltungsleistungen; Portalverbund (Abs. 5)

Art. 91c Abs. 5 GG begründet eine ausschließliche Gesetzgebungskompetenz des Bundes (mit Zustimmung des Bundesrats) für den übergreifenden informationstechnische Zugang zu Verwaltungsleistungen. Er begründet jedoch keine Verwaltungskompetenz zum Betrieb der IT-Systeme.[90] Die Reichweite betrifft primär Zugangskomponenten (Frontoffice/Portalverbund). Für reine interne Fachverfahren und Plattform-/Backoffice-Komponenten ist Abs. 5 regelmäßig nicht anwendbar, es sei denn, die konkrete Komponente fungiert als Basiskomponente des Portalverbunds.

Art. 91c Abs. 5 GG ist die Grundlage für das Onlinezugangsgesetz (OZG) des Bundes. Für OSiP ist dies nur insoweit relevant, als ggf. ein Onlinedienst iSd OZG angeboten werden soll, mit dem Einzelpersonen oder Unternehmen über das Internet Anträge auf eine ZSÜ stellen können (B.VI.1.). Ein solcher Onlinedienst ist von den dahinterliegenden Komponenten (Fachverfahren, OSiP-Transportinfrastruktur) zu trennen und nach der durch das OZG vorgegebenen Struktur aufzubauen. Datenschutzrechtlich ergibt sich für die OZG-Komponente durch § 8a OZG eine andere Verantwortungsverteilung als für OSiP im Übrigen. § 8a OZG schafft eine Rechtsgrundlage für die den Onlinedienst betreibende Stelle (§ 8a Abs. 1 OZG) und weist diese für die Verarbeitung innerhalb dieser Komponente die alleinige Verantwortlichkeit zu (§ 8a Abs. 4 OZG).

---

[90] BT-Drs. 18/12205, S. 9 f.

2.1.4. IT-Staatsvertrag (IT-StV)

Bund und Länder haben mit dem IT-StV die Möglichkeit des Art. 91c GG genutzt und eine Grundlage für die danach zulässige Kooperation geschaffen. Die damit geschaffene Struktur und die Beschlüsse des IT-Planungsrats schaffen im Ergebnis eine verbindliche Grundlage für OSiP, einschließlich der Ermöglichung eines zentralen IT-Betriebs.

2.1.4.1. Rechtsnatur von Staatsverträgen

Staatsverträge zwischen Bund und Ländern sind koordinationsrechtliche Vereinbarungen der beteiligten Verwaltungsträger. Innerstaatliche Bindungswirkung – also Wirkung gegenüber den öffentlichen Stellen in Bund und Ländern – entfalten sie erst durch die jeweiligen Zustimmungsgesetze von Bund und Ländern, durch die sie in deren innerstaatliches Recht „transformiert" werden. Mit der Transformation erlangen die Vertragsbestimmungen den Rang eines einfachen Gesetzes in der jeweiligen Rechtsordnung (des Bundes bzw. Landes). Sie stehen unterhalb des Grundgesetzes bzw. der Landesverfassung, aber neben sonstigem einfachen Gesetzesrecht. Die verfassungsrechtlichen Kompetenzgrenzen (Art. 30, 83 ff., 91c GG) bleiben durch Staatsverträge unberührt.

2.1.4.2. Wirkung des IT-StV und von Beschlüssen des IT-Planungsrats

Das Vorstehende gilt auch für den IT-Staatsvertrag („Vertrag zur Ausführung von Art. 91c GG" bzw. IT-StV). Dieser ist (inkl. Änderungsstaatsverträgen) in allen Ländern durch Zustimmungsgesetze in Kraft gesetzt worden. Für eine Übersicht der Ratifizierungsgesetze siehe Anlage 6. Durch die Zustimmungs- und Transformationsgesetze in Bund und Land erhält der IT-StV die Wirkung von einfachgesetzlichem Bundes- bzw. Landesrecht.

Diese Wirkung erfasst auch Beschlüsse des IT-Planungsrats (IT-PLR), soweit nachfolgend ausgeführt: Der IT-StV sieht vor, dass der IT-PLR Beschlüsse zu fachunabhängigen und fachübergreifenden Interoperabilitäts- und IT-Sicherheitsstandards fasst (§ 1 Abs. 1 Nr. 2 und § 2 IT-StV). Diese können zum einen mit einfacher Mehrheit als Empfehlungen für die öffentliche Verwaltung beschlossen werden (§ 2 Abs. 1 IT-StV und Anhang A, Teil B Ziffer 6, Spiegelstrich 1). Zum anderen können sie, soweit dies für den bund-länderübergreifenden Datenaustausch oder zur Vereinheitlichung des Datenaustauschs der öffentlichen Verwaltung mit Bürgen und Wirtschaft notwendig ist, unter den Voraussetzungen von § 2 Abs. 2 und Abs. 3 IT-StV auch als verbindliche Standards beschlossen werden. Dabei verlangt das Beschlussverfahren eine qualifizierte Mehrheit (§ 1 Abs. 7 und § 2 Abs. 2 IT-StV). Der Vertrag ordnet ausdrücklich an, dass die Beschlüsse

über verbindliche Standards Bindungswirkung entfalten und innerhalb der vom IT-PLR gesetzten Fristen von Bund und Ländern in ihren jeweiligen Verwaltungsräumen umgesetzt werden (§ 2 Abs. 2 Satz 2 IT-StV). Da das Beschlussverfahren und die Wirkung der Beschlüsse im IT-StV vereinbart sind, wird es von den Zustimmungsgesetzen der Länder erfasst und in Landesrecht transformiert. Zudem haben die Länder regelmäßig auch ausdrücklich angeordnet, dass die vom IT-PLR verbindlich (teils auch: als Empfehlung)[91] beschlossenen Interoperabilitäts- und IT-Sicherheitsstandards von den öffentlichen Stellen anzuwenden sind.[92] Soweit der IT-Planungsrat verbindliche Beschlüsse über IT-Interoperabilitäts- und IT-Sicherheitsstandards fasst, entfalten diese Beschlüsse für die betroffenen Verwaltungen von Bund und Ländern mithin Bindungswirkung mit Gesetzesrang.

Auf Beschlüsse über das Verbindungsnetz findet § 4 Abs. 3 IT-NetzG Anwendung (siehe auch § 7 Abs. 2 GO IT-PLR.

Für andere Beschlussgegenstände gelten die in § 7 Abs. 2 GO IT-PLR vorgesehenen, engeren Bindungsmechanismen (einstimmige Beschlüsse bzw. Beschlüsse, in denen vorgesehen ist, dass sie Bindungswirkung nur im Zuständigkeitsbereich der zustimmenden Gebietskörperschaften entfalten).

2.1.4.3. Umsetzung der IT-Kooperation auf Basis des IT-StV; FITKO

Wie gesehen ermöglicht Art. 91c GG in Verbindung mit dem IT-StV dem IT-PLR zum einen, Interoperabilitäts- und IT-Sicherheitsstandards verbindlich zu beschließen, und zum anderen, länderübergreifende E-Government-Projekte im Rahmen seiner Aufgaben als Produkt zu führen und zu steuern (§ 1 Satz 1 Nr. 4 IT-StV). Die FITKO ihrerseits unterstützt den IT-PLR bei der Erfüllung seiner Aufgaben organisatorisch und fachlich (§ 5 Abs. 1 Satz 2 IT-StV).

Gemäß § 5 IT-StV wurde zum 1. Januar 2020 die Föderale IT-Kooperation („FITKO“) als rechtsfähige Anstalt des öffentlichen Rechts in gemeinsamer Trägerschaft von Bund und Ländern mit Sitz in Frankfurt am Main errichtet.[93] Sie unterstützt den IT-PLR fachlich und organisatorisch und übernimmt nach seinen Beschlüssen die Umsetzung von Projekten und Produkten (§ 7 IT-

---

[91] Keine Differenzierung enthält z.B. jedenfalls dem Wortlaut nach Art. 51 Abs. 2 BayVwDiG.

[92] Vgl. etwa § 17 S. 1 EGovG BW.

[93] Grundlage: Erster IT-Änderungsstaatsvertrags vom 13. September 2019 (BGBl. I S. 1416).

StV). Sie verfügt nicht über eigene hoheitliche Befugnisse.[94] In diesem Zusammenhang sind folgende Beschlüsse des IT-PLR hervorzuheben:

- Gründungsbeschluss FITKO:[95] Errichtung, Aufgabenzuschnitt (u.a. Übernahme 115-Geschäftsstelle, GovData-Koordinierung, FIM/BFD), wirtschaftliche Steuerung, Aufgabenübertragung allein durch Beschluss des IT-Planungsrats (keine unmittelbare Delegation durch Einzelpartner).
- Übernahme von OSiP als Anwendung[96] und Eingliederung in das Produktportfolio[97] des IT-PLR bzw. der FITKO zum 01.02.2022.
- Mandat für OSiP-Neukonzeption:[98] Der IT-Planungsrat hat die FITKO mit Neukonzeption, Neuentwicklung und Roll-Out von OSiP beauftragt und die Zielvorgaben festgelegt. Dies ist die Grundlage der Zuständigkeits- und Auftragskette für einen möglichen zentralen Betrieb (iVm mit entsprechenden Nutzungsvereinbarungen).

Werden auf Basis der IT-Kooperation über den IT-PLR ebenenübergreifende IT-Verfahren – wie OSiP – betrieben und von öffentlichen Stellen genutzt, so verbleiben die Sachentscheidungen (nach dem jeweiligen Fachrecht) bei den zuständigen Behörden, sodass grundsätzlich kein Konflikt mit dem Verbot der Mischverwaltung entsteht. Dies gilt auch bei zentralen Betriebsmodellen. Die Zentralisierung des IT-Betriebs führt (grundsätzlich) nicht zu einer – unzulässigen – Zentralisierung von fachlichen Zuständigkeiten und Sachentscheidungen.

Rechtliche Folgen: Der IT-Staatsvertrag und die FITKO-Errichtung zeigen, dass das institutionelle Zusammenwirken (Abs. 1) praktisch über die gemeinsame Einrichtung operationalisiert werden soll. Zentrale Dienste wie OSiP lassen sich auf dieser Basis rechtlich in die föderale IT-Governance einbetten, ohne Vollzugsentscheidungen zu zentralisieren.

---

[94] Vgl. Gesetz zu dem Ersten IT-Änderungsstaatsvertrag vom 13. September 2019 (BGBl. I S. 1416); BeckOK GG/Wischmeyer Rn. 17.

[95] IT-PLR, Beschluss 2019/47 (30. Sitzung) vom 29.10.2019.

[96] IT-PLR, Beschluss 2017/12 (22. Sitzung) vom 22.03.2017.

[97] IT-PLR, Beschluss 2021/13 (34. Sitzung) vom 17.03.2021.

[98] IT-PLR, Beschluss 2025/20 (46. Sitzung) vom 26.03.2025.

2.1.5. Zwischenergebnis: Kooperationsformen für länderübergreifenden Dienst

Art. 91c GG eröffnet Bund und Ländern die Grundlage, bei Planung, Errichtung und Betrieb der für die Aufgabenerfüllung benötigten IT-Systeme zusammenzuwirken (Abs. 1) und hierfür Vereinbarungen – einschließlich gemeinschaftlichen Betriebs – zu schließen (Abs. 2, 3). Einfachrechtlich wird dies durch den IT-Staatsvertrag konkretisiert (IT-PL, Standardsetzung, Projektsteuerung), ohne die datenschutzrechtliche Verantwortlichkeit für fachliche Anwendungen bereits abstrakt festzulegen. Maßgeblich bleibt die konkrete Ausgestaltung des Dienstes und ggf. eine Regelung durch Beschlüsse des IT-PLR.

2.2. Grenze: Vermeidung unzulässiger Mischverwaltung

Verfassungsrechtlich zulässig ist der zentrale Betrieb, solange die FITKO keine hoheitlichen Entscheidungsbefugnisse über Durchführung oder Ergebnis der Sicherheits-/Zuverlässigkeitsprüfungen erhält. Die materiellen Entscheidungen verbleiben bei den jeweils zuständigen Behörden – die FITKO darf ausschließlich die technische Infrastruktur bereitstellen und (durch den IT-Dienstleister) betreiben.[99]

Diese Voraussetzung kann auch bei einem zentralen Betrieb, wie im Zielbild für das neue OSiP, gewahrt werden. Setzen Landes- oder Bundesbehörden OSiP ein, verbleiben die fachlichen Sachentscheidungen vollständig bei der jeweils zuständigen Bundesbehörde. Die FITKO erbringt eine kooperative IT-Infrastrukturleistung nach Art. 91c Abs. 1 und 3 GG und verlagert keine Vollzugszuständigkeiten. Soweit OSiP (oder ein vorgeschalteter Dienst) einen echten Frontoffice-Onlinedienst bereitstellt, greifen ausschließlich die Regelungen des Portalverbunds nach Art. 91c Abs. 5 GG und dem OZG. Das fachinterne Backoffice bleibt davon unberührt. Das Verbot der Mischverwaltung ist gewahrt; die Zurechenbarkeit der Entscheidungen bleibt eindeutig.

Hinsichtlich der Governance gilt, dass der IT-Planungsrat koordiniert und Standards setzt; die FITKO handelt als gemeinsame Einrichtung ohne eigene Hoheitsbefugnisse. Der Betrieb folgt dem Zielbild der Leistungsbeschreibung (Transportinfrastruktur und Fachverfahren mit Ende-zu-Ende-Verschlüsselung sowie Zero-Trust-Ansatz). Für Transportfunktionen ist Art. 91c Abs. 4 GG (Verbindungsnetz) zu beachten (1.2.3.2. und III.1.1.).

---

[99] Vgl. BeckOK GG/Heun, Art. 91c Rn. 17.

Die Verarbeitung personenbezogener Daten durch die FITKO bzw. den zentralen Betreiber sollte als Auftragsverarbeitung für die jeweils Verantwortlichen erfolgen (siehe II.1). Eine Kompetenzüberschreitung oder unzulässige Zentralisierung liegt hierin nicht.

2.3. Abgrenzung des Anwendungsbereichs des OZG

OSiP als solches ist keine OZG-Anwendung. Unter das OZG würde jedoch ein Antragsdienst fallen.

2.3.1. Geltung des OZG nur für OSiP-Antragsdienst

Das OZG erfasst Onlinedienste, d.h. insbesondere digitale Antragsdienste (über das Internet) mit Weiterleitung der Anträge an die zuständige Behörde und Rückkanal. Für länderübergreifend bereitgestellte Onlinedienste (Einer-für-Alle – EfA) ordnet § 8a Abs. 4 OZG der bereitstellenden Behörde die Verantwortlichkeit für den Onlinedienst zu; der technische Betrieb kann als Auftragsverarbeitung erfolgen. Fachanwendungen/Backoffice-Verfahren fallen demgegenüber nicht unter § 8a OZG.

Nur soweit ein Antragsassistent für Einzelpersonen/Unternehmen über das Internet bereitgestellt wird – was angedacht ist (Zielarchitektur und Grundprinzipien) – kann dieser Teil von OSiP (bzw. ein vorgeschalteter OSiP-Onlinedienst) als OZG-Anwendung zu qualifizieren sein. In diesem begrenzten Umfang greifen die Regelungen und die Verantwortlichkeitsverteilung gemäß § 8a OZG (getrennte Verantwortlichkeit: zentral betreibende Behörde für den Onlinedienst vs. Fachbehörde/Erkenntnisstelle für nachgelagerte OSiP-Verfahren).

2.3.2. Keine Geltung des OZG für OSiP im Übrigen

Für Dienste außerhalb des OZG (Fachanwendungen, Plattform-/Infrastrukturleistungen ohne Frontoffice, Transportinfrastruktur) kommt § 8a OZG nicht zur Anwendung. Auch eine analoge Anwendung von § 8a OZG scheidet in diesem Fall aus. § 8a ist auf Art. 91c Abs. 5 GG und damit auf den Portalverbund bezogen; die Regelung verfolgt somit einen ganz eigenen Zweck, der für die Übrigen Komponenten von OSiP nicht eingreift.

Für die übrigen Komponenten, die nicht unter das OZG fallen, bestimmt – wie sonst auch bei Kooperationen nach Art. 91c GG – das Kooperations-/Betriebsmodell die Rollenverteilung (soweit, wie bei OSiP außerhalb von § 8a OZG, keine Spezialregelungen bestehen). Auszugehen ist dabei von der alleinigen Verantwortlichkeit der nutzenden Behörden für das Fachverfahren und von dem Grundsatz, dass IT-Betreiber als Auftragsverarbeiter agieren (müssen), sofern – wie bei

OSiP – nichts anderes durch Rechtsvorschrift geregelt ist. Die Zuweisung der Verantwortlichkeit kann durch Staatsverträge oder Verwaltungsvereinbarungen konkretisiert werden. Wo keine spezialgesetzliche Zuweisung besteht, ist regelmäßig für die IT-Dienstleistung eine Auftragsverarbeitungsvereinbarung angezeigt (dies schon deshalb, da es dem IT-Dienstleister dann an einer Rechtsgrundlage für die eigenverantwortliche Verarbeitung fehlt).

Folgen für OSiP/FITKO: Der zentrale Betrieb von OSiP als fachliche Basis-/Plattformleistung lässt sich über Art. 91c GG (i. V. m. IT-Staatsvertrag) rechtssicher kooperativ organisieren. OZG-Bezug entsteht nur dort, wo ein Antragsassistent bereitgestellt wird (OSiP-Antragslösung für Unternehmen oder Einzelpersonen). Für den reinen Plattform-/Backoffice-Betrieb greift § 8a OZG nicht.

2.4. Ergebnis

Unter den skizzierten Voraussetzungen ist ein zentraler Betrieb von OSiP durch die FITKO verfassungs- und datenschutzrechtlich zulässig.

Verfassungsrechtlich stützt sich der zentrale Betrieb auf Art. 91c Abs. 1 GG, den IT-StV und die Beschlüsse des IT-PLR. Das Verbot der Mischverwaltung wird gewahrt, solange die fachlichen Sachentscheidungen bei den zuständigen Behörden verbleiben und die FITKO (bzw. der zentrale IT-Dienstleister) ausschließlich technische Unterstützungsleistungen erbringt. Der Beschluss 2025/20 bestätigt das föderale Mandat für die OSiP-Neukonzeption.

Datenschutzrechtlich können die das Verfahren nutzenden Behörden (die für ZSÜ zuständigen Stellen und die Erkenntnisstellen) die FITKO bzw. den zentralen IT-Dienstleister nach den Regeln des Datenschutzrechts als Auftragsverarbeiter beauftragen. Dabei ist ein zentraler Betrieb zulässig, soweit die datenschutzrechtlichen Voraussetzungen – weisungsabhängig Verarbeitung, strikte Mandantentrennung – gewahrt werden.

3. Zu beachtende föderale Besonderheiten bei zentralem Betrieb

Frage: „*Welche föderalen Unterschiede oder Besonderheiten könnten einem zentralen Betrieb entgegenstehen?*"

Kurzantwort:

Der zentrale Betrieb von OSiP ist verfassungsrechtlich zulässig (siehe C I. 2.), erfordert aber eine technisch anpassbare (parametrisierbare) Zielarchitektur, um föderale Divergenzen im Datenschutz- und Verfahrensrecht der Länder abzubilden.

Zu beachtende Besonderheiten bestehen u.a. in folgenden Bereichen:

1. Organisatorische Trennung der zuständigen Stellen: In den SÜG verlangen der Bund und mehrere Länder eine innerbehördliche organisatorische Abgrenzung der Sicherheitsüberprüfungsstelle. Dies erfordert eine strikte Mandantentrennung und ein entsprechendes Berechtigungssystem.
2. Unterschiedliche Lösch- und Aufbewahrungsfristen: Länderrechtlich abweichende Lösch- und Aufbewahrungsfristen, Dokumentations- und Übermittlungspflichten sowie enge Weiterverwendungs- und Empfängerkreise verlangen länderbezogene Aufbewahrungs- und Zweckbindungs-Policies einschließlich revisionsfester Protokollierung.
3. Sonderregime für nichtöffentliche Stellen: Für industrielle Auftragnehmer und VS-Verarbeiter gelten in vielen Ländern eigenständige Verfahrens-, Rollen- und Zuständigkeitsmodelle. Erforderlich sind separate Tenants/Scopes, spezifische Rollen (z.B. Sicherheitsbevollmächtigte) und eine konfigurierbare Ausnahmesteuerung für Mitwirkungs- und Verarbeitungspflichten.

Diese Besonderheiten sind systemseitig umzusetzen. Sie stehen dem zentralen Betrieb jedoch nicht entgegen.

Ein zentraler Betrieb von OSiP ist verfassungs- und datenschutzrechtlich zulässig (siehe C I 2.1), setzt jedoch eine Zielarchitektur voraus, die landesspezifische Verfahrens- und Organisationsbesonderheiten abbildet. Eine wesentliche landes- und bundesrechtliche Anforderung sowie die daraus abgeleiteten System-Vorgaben sind in Anlage 4 zusammengefasst. Eine vollständige Erfassung ist im Rahmen der Anforderungsdefinitionen für die einzelnen OSiP-Anwendungsfälle durch die beteiligten Stakeholder zu gewährleisten.

Die hier vorgenommene Prüfung erfasst die zuvor genannten Regelungen (siehe C. I. 1) und bewertet sie danach, ob sie föderale Divergenzen begründen, die einen zentralen Betrieb beeinträchtigen können.

Ein erhöhtes Konfliktpotenzial findet sich vor allem in den Landes-Sicherheitsüberprüfungsgesetzen (insbesondere bei organisatorischen Trennungsanforderungen, der Löschfristen und den Sonderregimen für nichtöffentliche Stellen) und punktuell in fachrechtlichen Sonderregimen (z.B. im Justizvollzug einzelner Länder). Demgegenüber sind Bundesgesetze, wie Luftsicherheits- und Hafensicherheitsrecht, unions- bzw. bundeseinheitlich vorgeprägt. Relevante föderale Unterschiede ergeben sich dort primär aus den Landes-Hafensicherheitsgesetzen. Einzelheiten, einschließlich konkreter Normnachweise und Beispiele, enthält Anlage 4.

Fragen bezüglich der Einholung von Zustimmungen und Formvorschriften zur Durchführung der Sicherheitsüberprüfung werden in C II.7 erörtert. Auf die Anforderungen zur IT-Sicherheit wird in C II 4.2.1 eingegangen.

Im Ergebnis ist ein zentraler Betrieb von OSiP verfassungsrechtlich möglich, setzt aber eine parametrisierbare Zielarchitektur voraus, die die landesrechtlichen Besonderheiten organisations-, verfahrens- und aktenrechtlich abbildet.

Zusammengefasst sind die folgenden Anforderungen bei der Gestaltung der zentralen OSiP-Zielarchitektur zwingend zu beachten:

3.1. Organisatorische Trennung der „zuständigen Stelle“

Mandantenfähigkeit und -trennung sind eine verfassungs- und datenschutzrechtliche abzuleitende Grundanforderung für ein zentral betriebenes OSiP-System (2.4.). Die Anforderungen an IT-Verfahren zur Unterstützung von ZSÜ sind durch fachgesetzliche Regelungen insoweit teils besonders strikt.

Mehrere Länder verlangen die innerbehördliche organisatorische Abgrenzung der für ZSÜ zuständigen Stelle insbesondere gegenüber der Personalverwaltung (in einzelnen Ländern zusätzlich gegenüber behördlichem Datenschutzbeauftragten und Antikorruptionsstelle). Ein zentraler Betrieb muss dies abbilden und ist daher nur tragfähig, wenn OSiP klare Trennungen technisch ermöglicht (Mandantenfähigkeit, granulare Rollen- und Rechtekonzepte, getrennte Work-Queues und Organisationsobjekte je Land, Behörde und innerbehördlich zuständiger Abteilung).

3.2. Empfängerkreise & Zweckbindung (Übermittlungsrestriktionen)

Landesrecht sieht teils vor, dass Übermittlungen ausschließlich an öffentliche Stellen zulässig sind und Zusatz- bzw. Weiterverwendungszwecke eng definiert werden (z.B. für Disziplinar-/UA-Zwecke). OSiP muss dies in geeigneter Weise unterstützen. Eine Weitergabe an Private ist – wo bundes- oder landesrechtlich untersagt – systemseitig auszuschließen. Entsprechende Maßnahmen könnten sein: Empfänger-Whitelists, Zweck-/Verwendungsfilter und vorgangsbezogene Freigabeprozesse je Landesprofil.

Es sprechen jedoch gute Gründe dafür, dass das Verbot der Übermittlung an nicht-öffentliche Stellen dem Einsatz eines nicht-öffentlichen IT-Dienstleisters nicht entgegensteht, wobei in diesem Fall eine Ende-zu-Ende-Verschlüsselung erst Recht zu empfehlen ist (siehe hierzu im Einzelnen 1.1.2.2.2.)

3.3. Sonderregime für nichtöffentliche Stellen

Mehrere Länder statuieren für nichtöffentliche Stellen (z.B. industrielle Auftragnehmer) eigenständige Akten-, Zuständigkeits- und Rollenmodelle; teils werden sie datenschutzrechtlich wie öffentliche Stellen behandelt. Ein zentraler Betrieb erfordert entsprechend spezifische Rollen (z.B. Sicherheitsbevollmächtigte/r) und Workflows.

3.4. Akten-/Dateienregime und Aufbewahrung/Löschung

Vorgaben zu eigener Sicherheitsakte, strikter Trennung von Sicherheits- und Personalakten, Sperr-/Vernichtungsregeln, Übermittlungs- und Dokumentationspflichten sowie abweichenden Aufbewahrungs- und Löschfristen differieren zwischen den Ländern. OSiP muss entsprechende Löschregeln, Sperr-/Vernichtungs-Workflows, Transfer-/Abgabemechanismen (z.B. bei Zuständigkeits- oder Dienstherrenwechsel) und revisionsfeste Übermittlungsprotokollierung bereitstellen.

3.5. Variable Zuständigkeiten und Verwaltungsvorschriften

Zuständigkeiten können landesrechtlich – teils per Rechtsverordnung – unterschiedlich festgelegt und geändert werden (mehrstufige Kaskaden bis zur Ministeriumsebene). Der zentrale Betrieb sollte dies unter strikter Wahrung der Zuständigkeiten in geeigneter Weise unterstützen, z.B. durch (Bereitstellung oder Anbindung an) pflegbare Behörden- und Zuständigkeitsverzeichnisse sowie parametrisierbare Absender-/Siegel-/Mitwirkungsangaben je Land.

3.6. Folgen für die zentrale Betriebsform

Ohne die vorstehenden skizzierten Funktionen und Parametrisierungen drohen Rechtsverstöße (insbesondere unzulässige Übermittlungen, Organisationsverstöße, Fristversäumnisse, überlange Speicherung etc.) oder nur eingeschränkte Beitritts- bzw. Nutzungsoptionen einzelner Länder. Werden die länderspezifischen Besonderheiten hingegen systemseitig um- und durchgesetzt, so stehen sie der Rechtmäßigkeit eines zentralen Betriebs nicht entgegen.

II. Datenschutz und IT-Sicherheit

1. Verantwortlichkeitsmodell

Frage: *„Welche Konstellation der datenschutzrechtlichen Verantwortlichkeit (alleinige Verantwortlichkeit der FITKO, gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO, Auftragsverarbeitung gem. Art. 28 DSGVO) ist für die Zielarchitektur rechtlich möglich und empfehlenswert? Welche Vor- und Nachteile ergeben sich jeweils?"*

Kurzantwort:

Das zu empfehlende und rechtlich tragfähigste Modell ist die Auftragsverarbeitung der FITKO (Art. 28 DSGVO) mit dem IT-Dienstleister als Unterauftragnehmer.

Die FITKO sollte bei der Bereitstellung der OSiP-Transportinfrastruktur und des Backoffice-Dienstes zwingend als Auftragsverarbeiterin der nutzenden Stellen tätig werden. Eine alleinige oder gemeinsame Verantwortlichkeit der FITKO für die Verarbeitung von Daten in OSiP würde eine datenschutzrechtliche Rechtsgrundlage voraussetzen, die – nach derzeitigem Stand – nicht ersichtlich ist.

Zu empfehlen ist zudem eine Ende-zu-Ende-Verschlüsselung (E2EE), um die Verarbeitung von Inhaltsdaten durch den IT-Dienstleister vollständig auszuschließen (und damit ggf. sogar die Geltung des Datenschutzrechts für das Outsourcing).

Die nutzenden Stellen sollten dementsprechend als (untereinander getrennt) Verantwortliche für die im Rahmen ihrer jeweiligen Aufgaben mit OSiP verarbeiteten Daten auftreten.

Im Folgenden wird das Konzept der datenschutzrechtlichen Verantwortlichkeit mit den möglichen Varianten erläutert (1.1.) und dann auf die bei OSiP auftretenden Verarbeitungsvorgänge angewendet (1.2.).

1.1. Bestimmung der Verantwortlichkeit („Wer ist verantwortlich?")

Datenschutzrechtliche Verantwortlichkeit bezieht sich stets auf konkrete, dem Datenschutzrecht unterliegende Verarbeitungsvorgänge. Hierzu und zur Anwendung auf OSiP siehe 1.2.

Für jeden Verarbeitungsvorgang gibt es nach der DSGVO mindestens eine Stelle, die als Verantwortlicher bezeichnet wird (Art. 4 Nr. 7 DSGVO). Sie muss sicherstellen, dass eine Rechtsgrundlage für die Verarbeitung besteht, ist zur Einhaltung der Datenschutzgrundsätze bei der Verarbeitung verpflichtet und muss dies nachweisen können (Art. 5 DSGVO).[100]

Zum Verantwortlichen wird eine Stelle entweder, indem sie die Zwecke und Mittel der Verarbeitung bestimmt, oder indem eine Rechtsvorschrift sie als Verantwortlichen benennt. Treffen diese Voraussetzungen für denselben Verarbeitungsvorgang auf mehrere Stellen zu, sind diese gemeinsam verantwortlich.

Von der Rolle als Verantwortlicher abzugrenzen ist die weisungsgebundene Durchführung einer Datenverarbeitung im Auftrag einer anderen Stelle als Auftragsverarbeiter.

1.1.1. Begriff des Verantwortlichen

Der Begriff des Verantwortlichen (Art. 4 Nr. 7 DSGVO) ist weit auszulegen.[101] So wird sichergestellt, dass es für jede Verarbeitung mindestens einen Verantwortlichen gibt, gegen den die von der Verarbeitung betroffenen Personen ihre Rechte nach der DSGVO durchsetzen können. Um für eine Verarbeitung als Verantwortlicher in Frage zu kommen, muss eine Stelle lediglich rechtlich und tatsächlich in der Lage sein, diesbezüglich die Pflichten nach der DSGVO zu erfüllen – sie muss aber nicht zwingend eigene Rechtspersönlichkeit besitzen.[102] Insbesondere können Behörden bereits nach dem Wortlaut der DSGVO Verantwortliche sein.[103]

Konkret nennt Art. 4 Nr. 7 DSGVO zwei Wege, auf denen eine datenverarbeitende Stelle zum Verantwortlichen werden kann: Entweder sie legt die Zwecke und Mittel der Verarbeitung fest oder sie wird durch Rechtsvorschrift als Verantwortlicher für diese Verarbeitung benannt.

1.1.1.1. Verantwortlichkeit durch eigene Zwecksetzung

Wer – allein oder gemeinsam mit anderen – die Zwecke und Mittel der Verarbeitung bestimmt, wird dadurch zum Verantwortlichen (Art. 4 Nr. 7, 1. Halbsatz DSGVO). Für das „Bestimmen von

---

100 EuGH, Urt. v. 11.01.2024, C-231/22 – „État belge", Rn. 41.

101 EuGH, Urt. v. 11.01.2024, C-231/22 – „État belge", Rn. 28 m.w.N.

102 EuGH, Urt. v. 27.02.2025, C-638/23 – „Amt der Tiroler Landesregierung", Rn. 30; Urt. v. 11.01.2024, C-231/22 – „État belge", Rn. 36.

103 Neben der Behörde soll der Behördenleiter selbst Verantwortlicher sein, s. BeckOK-DSR/*Schild*, 52. Ed., Art. 4 DSGVO 89 mit Hinweis auf OLG Dresden, ZD 2022, 159.

Zwecken und Mitteln“ ist entscheidend, dass die Person oder Stelle aus Eigeninteresse auf die Verarbeitung der Daten Einfluss nimmt.[104] Zur Möglichkeit, dass zwei oder mehr Stellen die Zwecke und Mittel gemeinsam festlegen („Gemeinsame Verantwortlichkeit“, Art. 26 DSGVO), siehe cc).

1.1.1.2. Benennung des Verantwortlichen durch Rechtsvorschrift

Statt durch Festlegung von Zweck und Mittel (s.o.) kann eine Stelle auch dadurch datenschutzrechtliche Verantwortliche werden, dass sie durch Rechtsnorm als solche benannt wird (Art. 4 Nr. 7, 2. Halbsatz DSGVO). In diesem Fall müssen die Zwecke und Mittel der Verarbeitung rechtlich vorgegeben sein. Hingegen muss die Behörde nicht über die Zwecke und Mittel der Verarbeitung entscheiden.[105] Sie muss lediglich in der Lage sein, die Pflichten zu erfüllen, die sich aus der Stellung als Verantwortlicher ergeben (s.o.).

Für die Benennung als Verantwortlicher durch Rechtsvorschrift genügt es, dass die entsprechenden Rechtsvorschriften die Zwecke und Mittel der Verarbeitung, den Umfang der Verarbeitung und die Einordnung der Stelle als Verantwortlicher nicht ausdrücklich, sondern nur implizit vorgeben.[106] Die Benennung als Verantwortlicher muss sich aber „mit hinreichender Bestimmtheit aus der Rolle, dem Auftrag und den Aufgaben der betroffenen Person oder Einrichtung“ ergeben.[107] Es ist davon auszugehen, dass die Aufgabenzuweisung an eine Behörde in der Regel die Verantwortlichkeit für die zur Aufgabenerfüllung erforderliche Datenverarbeitung impliziert.[108]

1.1.2. Gemeinsame Verantwortlichkeit

Wenn zwei oder mehr Stellen die Zwecke und Mittel der Verarbeitung gemeinsam festlegen, ist jede dieser Stellen nach Art. 4 Nr. 7, 1. Halbsatz DSGVO verantwortlich (siehe Art. 26 Abs. 1 Satz 1 DSGVO). Soweit für eine Verarbeitung eine gemeinsame Verantwortlichkeit besteht, benötigt jeder der gemeinsam Verantwortlichen eine Rechtsgrundlage für die Verarbeitung und

---

104 EuGH, Urt. v. 05.12.2023, C-638/21 – „Nacionalinis visuo menes sveikatos centras“, Rn. 30 m.w.N.

105 EuGH, Urt. v. 27.02.2025, C-638/23 – „Amt der Tiroler Landesregierung“, Rn. 46; Urt. v. 11.01.2024, C-231/22 – „État belge“, Rn. 37 f.

106 EuGH, Urt. v. 27.02.2025, C-638/23 – „Amt der Tiroler Landesregierung“, Rn. 41.

107 EuGH, Urt. v. 27.02.2025, C-638/23 – „Amt der Tiroler Landesregierung“, Rn. 28; Urt. v. 11.01.2024, C-231/22 – „État belge“, Rn. 36.

108 EDSA, Leitlinien 1/2020, V1.0, Rn. 22.

unterliegt den Pflichten nach der DSGVO, d.h. er muss die Einhaltung der Verarbeitungsgrundsätze sicherstellen.

Die „gemeinsame Verantwortlichen" müssen zudem eine Vereinbarung schließen, um die Erfüllung der DSGVO-Pflichten im Innenverhältnis aufzuteilen (Art. 26 DSGVO). Die Prüfung, ob bezüglich einer konkreten Verarbeitung eine gemeinsame Festlegung von Zwecken und Mitteln vorliegt, ist in der Praxis regelmäßig mit Unsicherheiten verbunden. Es bedarf einer Gesamtbetrachtung der tatsächlichen Umstände des Einzelfalls. Die aus der EuGH-Rechtsprechung ableitbaren Kriterien sind dabei ebenso weit gefasst wie unscharf. So kann eine Stelle selbst dann gemeinsam Verantwortlicher sein, wenn sie keine Zugriffsmöglichkeit auf die Daten hat.[109]

Auch Verantwortliche, die nach Art. 4 Nr. 7, 2. Halbsatz DSGVO durch Rechtsvorschrift bestimmt werden, können gemeinsam verantwortlich sein. Dies ist der Fall, wenn sich aus der Vorgabe der Zwecke und Mittel der Verarbeitung durch das Recht eine Verbindung der Verarbeitungsvorgänge mit gemeinsamer Verantwortlichkeit ergibt.[110] Denkbar ist auch eine „gemischte" gemeinsame Verantwortlichkeit, bei der eine Stelle nach Gesetz als Verantwortlicher benannt ist (Art. 4 Nr. 7, 2. Halbsatz DSGVO) und die andere Stelle Zwecke und Mittel der Verarbeitung bestimmt (Art. 4 Nr. 7, 1. Halbsatz DSGVO).[111]

Erste Ansatzpunkte: Analyse der Rollenmodelle nach Art. 4 Nr. 7, 26, 28 DSGVO; Bewertung der praktischen Konsequenzen für Steuerung, Haftung, Betroffenenrechte.

1.1.3. Auftragsverarbeitung

Von der Rolle als Verantwortlicher abzugrenzen ist der Fall, dass eine Stelle personenbezogene Daten nicht eigenverantwortlich, sondern im Auftrag des Verantwortlichen nach dessen Weisungen verarbeitet. Sie ist dann Auftragsverarbeiter (gem. Art. 4 Nr. 8 und Art. 28 DSGVO); der Auftraggeber ist Verantwortlicher.

Ein Tätigwerden als Auftragsverarbeiter ist typisch für IT-Dienstleister, die im Rahmen von Hosting, Wartung, oder Support personenbezogene Daten verarbeiten; ebenso für IT-Consultants, die Aufgaben wie Customizing und Implementierung übernehmen und dabei Zugriff auf personenbezogene Daten haben. Dies gilt unabhängig davon, ob die IT-Dienstleistung durch

---

109 EuGH, Urt. v. 29.7.2019, C-40/17 – „Fashion ID", Rz. 69.

110 EuGH Urt. v. 11.01.2024, C-231/22 – „État belge", Rz. 49.

111 EuGH, Urt. v. 27.02.2025, C-638/23 – „Amt der Tiroler Landesregierung", Rn. 48.

eine nichtöffentliche Stelle erbracht wird oder sie durch eine öffentliche Stelle einer anderen öffentliche Stelle bereitgestellt wird; in beiden Fällen kann also eine Auftragsverarbeitung vorliegen.

Merkmal	Auftragsverarbeiter (Art. 28 DSGVO)	Verantwortlicher (Art. 24 DSGVO)
Entscheidungsgewalt	Handelt weisungsgebunden im Auftrag des Verantwortlichen. Entscheidet nicht über Zwecke und wesentliche Mittel der Verarbeitung.	Entscheidet (allein oder gemeinsam mit anderen) über die Zwecke und Mittel der Datenverarbeitung. Hat die "Datenhoheit".
Zweck der Verarbeitung	Verarbeitet Daten ausschließlich für die vom Verantwortlichen vorgegebenen Zwecke.	Legt die Zwecke der Datenverarbeitung selbst fest und verfolgt eigene Interessen.
Verantwortung & Haftung	Trägt eine eingeschränkte Verantwortung. Haftet primär bei Missachtung der Weisungen oder bei Verstößen gegen spezifische Pflichten für Auftragsverarbeiter.	Trägt die Gesamtverantwortung für die Rechtmäßigkeit der Datenverarbeitung. Ist der primäre Ansprechpartner für Betroffene und Aufsichtsbehörden.
Rechtsgrundlage	Die Zusammenarbeit erfordert einen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO, der die Rechte und Pflichten regelt.	Benötigt für die Datenverarbeitung eine Rechtsgrundlage nach Art. 6, 9 und 10 DSGVO (z.B. Einwilligung, Vertragserfüllung).
Beziehung	Steht in einem Unterordnungsverhältnis zum Verantwortlichen ("verlängerter Arm").	Agiert eigenständig. Kann andere als Auftragsverarbeiter oder als gemeinsame Verantwortliche einbeziehen.

Beispiele	Ein externes IT-Systemhaus oder RZ-Betreiber (z.B. Dataport), das die Server und Fachanwendungen für eine Behörde wartet und betreibt. Externe Druckerei, Scandienstleister, SaaS-Anbieter.	Behörde, die personenbezogene Daten im Rahmen ihrer Aufgabenerfüllung verarbeitet.

1.1.4. Vor- und Nachteile

Getrennte Verantwortlichkeit, gemeinsame Verantwortlichkeit und Auftragsverarbeitung haben Rechtsfolgen und praktische Konsequenzen, die als Vor- oder Nachteile empfunden werden können. Als typisch sind zu nennen:

Verantwortungsmodell	Mögliche Vorteile	Mögliche Nachteile
Getrennte Verantwortlichkeit	- Klare Zuständigkeiten - Keine Haftung für Fehler anderer - Geringerer Abstimmungsaufwand (keine formelle Vereinbarung über die Aufteilung der Pflichten) - Hohe Autonomie	- Rechtsgrundlage für alle Beteiligten erforderlich
Gemeinsame Verantwortlichkeit	- Pflichten können im Innenverhältnis aufgeteilt werden (= Synergien z.B. durch zentrale Anfertigung einer DSFA) - (Aus Betroffenensicht:) Betroffene können sich an alle Beteiligten halten	- Rechtsgrundlage für alle Beteiligten erforderlich - Haftung für Mit-Verantwortliche im Außenverhältnis - Regelungsaufwand (Art. 26 DSGVO) - Erhöhter Koordinationsaufwand (kontinuierliche Abstimmung) - (Aus Beteiligtensicht:) Betroffene können sich an alle Beteiligten wenden

Auftragsverarbeitung	- Klare Hierarchie und Verantwortung - Keine gesonderte Rechtsgrundlage für Auftragsverarbeiter erforderlich („Privilegierte Datenweitergabe") - (Für Auftragnehmer:) reduzierte Haftung	- Sorgfalts- und Kontrollpflichten - (Für Verantwortlichen:) Haftung im Außenverhältnis - Bürokratischer Aufwand: Für jede Beauftragung muss ein AV-Vertrag geschlossen werden.

1.2. Verarbeitungsvorgänge („Wofür ist jemand verantwortlich?")

Datenschutzrechtliche Verantwortlichkeit bezieht sich stets auf konkrete, dem Datenschutzrecht unterliegende Verarbeitungsvorgänge. Vor der Prüfung der Verantwortlichkeit im Fall von OSiP ist daher zunächst festzustellen, inwieweit bei diesem Verfahren personenbezogene Daten verarbeitet werden.

Im zweiten Schritt ist dann festzustellen, wer dafür verantwortlich ist. Für OSiP können vereinfacht folgende Tätigkeiten unterschieden werden:

- Organisatorische Bereitstellung (1.2.1)
- Technische Bereitstellung (1.2.2)
- Nutzung (1.2.3)

1.2.1. Organisatorische Bereitstellung

Die organisatorische Bereitstellung ist für OSiP durch den Auftrag des IT-PLR als Aufgabe der FITKO zugewiesen (und wird von ihr selbst oder in ihrem Auftrag durch Dienstleister durchgeführt). Sie umfasst Tätigkeiten wie Konzeption, Entwicklung, Bedarfsplanung, Beratung und Koordinierung. Von den genannten Tätigkeiten zu trennen sind Aufgaben der technischen Bereitstellung, d.h. des IT-Betriebs, der die eigentliche Datenverarbeitung im produktiven Betrieb umfasst (1.2.2.).

Die genannten Aufgaben der organisatorischen Bereitstellung werden voraussichtlich zum Teil unmittelbar von der FITKO durchgeführt, soweit es um Steuerung, Konzeption, Definition der Anforderungen und Produktverantwortung geht. Entwicklungsaufgaben werden ggf. auf einen IT-Dienstleister übertragen. Die technische Bereitstellung soll in jedem Fall auf einen (weiteren) IT-Dienstleister übertragen werden.

Aus Datenschutzsicht ist zunächst zu prüfen, ob im Rahmen der genannten organisatorischen Tätigkeiten personenbezogene Daten verarbeitet werden und somit das Datenschutzrecht darauf anwendbar ist. Während die technische Bereitstellung üblicherweise zwingend mit der Verarbeitung personenbezogener Daten verbunden ist, ist dies bei der organisatorischen Bereitstellung, soweit sie sich auf Konzeptions- und Entwicklungstätigkeiten beschränkt, nicht zwingend der Fall. Zum Beispiel können die Konzeption und auch erste Entwicklungsarbeiten in der Regel ohne Verarbeitung personenbezogener Daten vorgenommen werden. Auch während der Produktivphase können steuernde Funktionen teilweise auf der Basis aggregierter (nicht-personenbezogener) Informationen erfüllt werden. Je näher die Tätigkeiten an die Vorbereitung oder Begleitung eines produktiven Betriebs gehen, umso eher werden erfahrungsgemäß jedoch auch personenbezogene Daten im Rahmen der organisatorischen Bereitstellung verarbeitet. Typischerweise betrifft dies Kontaktdaten der beteiligten Ansprechpartnerinnen und Ansprechpartner (z.B. Name, Funktion, dienstliche Kontaktdaten), Benutzerkennungen, Rollen- und Berechtigungsinformationen sowie zugehörige Protokolldaten im Rahmen von Tests, Fehleranalysen oder Supportfällen und in Ausnahmefällen Inhalte aus Test- oder Pilotdatensätzen, sofern nicht ausschließlich synthetische oder anonymisierte Testdaten eingesetzt werden.

Soweit personenbezogene Daten verarbeitet werden, muss ein Verantwortlicher bestimmt werden, der für die datenschutzrechtlichen Pflichten primär verantwortlich ist. Prinzipiell kann eine organisatorisch bereitstellende Stelle (1) allein verantwortlich, (2) gemeinsam verantwortlich mit der nutzenden Stelle oder (3) als Auftragsverarbeiterin der nutzenden Stelle handeln.

Dabei macht es datenschutzrechtlich einen erheblichen Unterschied, ob es sich lediglich um Daten z.B. von Testnutzern handelt, oder ob auch inhaltliche Daten (z.B. von Personen, die einer ZSÜ unterzogen werden) verarbeitet werden:

- Im ersten Fall erscheint es ggf. vertretbar, dass die FITKO diese Tätigkeiten im Rahmen der ihr zugewiesenen Aufgaben – namentlich auf Grundlage der Beschlüsse des IT-PLR und der datenschutzrechtlichen Generalnorm (für die FITKO also § 3 HDSIG iVm § 6 Abs. 3 IT-StV) – eigenverantwortlich durchführen könnte.[112] Soweit in dieser Phase ausschließlich anonymisierte oder vollständig synthetische Testdaten verwendet werden,

[112] Die Rechtsgrundlage für die Datenverarbeitung durch die FITKO ist insofern die Generalnorm des hessischen LDSG in Verbindung mit der der FITKO zugewiesenen Aufgabe, also § 3 Abs. 1 HessDSIFG (iVm § 6 Abs. 3 IT-StV) iVm § 5 Abs. 1 IT-StV iVm den entsprechenden Beschlüssen des IT-PLR zu Neukonzeption und Bereitstellung von OSiP.

ist der Anwendungsbereich der DSGVO nicht eröffnet; sobald hingegen personenbezogene Daten (einschließlich pseudonymisierter Testdaten mit Re-Identifikationsmöglichkeit) verarbeitet werden, findet die DSGVO für die FITKO unmittelbar Anwendung. Die Ausnahmen des Art. 2 Abs. 2 Buchst. a und d DSGVO (nationale Sicherheit bzw. Justiz/Strafverfolgung) greifen für die FITKO selbst regelmäßig nicht, da ihre Tätigkeiten auf die organisatorische und technische Unterstützung der ZSÜ-Verfahren gerichtet sind und nicht auf die originäre Wahrnehmung nachrichtendienstlicher oder strafverfolgender Aufgaben; insoweit verbleibt es bei der allgemeinen Anwendbarkeit von DSGVO und HDSIG.

- Im zweiten Fall – also soweit die FITKO oder von ihr beauftragte Dienstleister auch Einsicht in inhaltliche Daten aus konkreten ZSÜ-Verfahren erhalten (zu den o.g. genannten organisatorischen Zwecken wie Entwicklung, Beratung, Bedarfsplanung)– läge jedoch ein schwerwiegender Eingriff in die Grundrechte der Betroffenen vor, der eine spezifische Rechtsgrundlage erfordern würde. Denn nach allgemeiner Ansicht können schwerwiegende Eingriffe nicht auf die datenschutzrechtliche Generalnorm gestützt werden. Eine solche spezifische datenschutzrechtliche Rechtsgrundlage für die FITKO ist nicht ersichtlich (freilich könnte ein solche Norm theoretisch geschaffen werden). Daher bleibt insofern de lege lata nach hier vertretener Auffassung für eine solche Verarbeitung nur das Modell einer Auftragsverarbeitung.

1.2.2. Technische Bereitstellung

Die technische Bereitstellung erfasst typischerweise Hosting, Wartung und Support. Diese Aufgaben werden regelmäßig durch spezialisierte IT-Dienstleister erbracht (IT-Outsourcing). Neben privaten Dienstleistern gibt es in Bund, Ländern und Kommunen öffentliche IT-Dienstleister in diversen Organisationsformen. Im Fall von OSiP soll die technische Bereitstellung durch einen Dienstleister im Auftrag der FITKO erbracht werden.

1.2.2.1. Grundsatz: Technische Bereitstellung als Auftragsverarbeitung

IT-Dienstleister der öffentlichen Verwaltung werden typischerweise als Auftragsverarbeiter der nutzenden Stelle tätig. Dies ist jedoch nicht immer der Fall, denn zum Teil ist die datenschutzrechtliche Verantwortlichkeit für die Erbringung bestimmter Dienstleistungen gesetzlich einer anderen Stelle oder dem technischen Dienstleister selbst zugewiesen. Für den OSiP-Betrieb ist allerdings keine besondere Zuweisung der Verantwortlichkeit einschlägig.

Für die technische Bereitstellung ergibt sich, dass es weder eine gesonderte Zuweisung von datenschutzrechtlicher Verantwortlichkeit an die FITKO (oder einen IT-Dienstleister) noch eine Rechtsgrundlage gibt, auf der die FITKO (oder ein IT-Dienstleister) inhaltliche Daten aus ZSÜ eigenverantwortlich verarbeiten dürfte. Die vorhandenen Rechtsgrundlagen der FITKO (siehe 1.2.1.) decken eine solche Verarbeitung nicht. Daher bleibt insofern de lege lata nach hier vertretener Auffassung für eine solche Verarbeitung nur das Modell einer Auftragsverarbeitung.[113]

Eine Auftragsverarbeitung ist jedoch streng genommen nur insoweit erforderlich, als überhaupt personenbezogene Daten verarbeitet werden. Bricht man die Verarbeitungsvorgänge im Rahmen der technischen Bereitstellung weiter herunter, so ist dies ggf. nicht der Fall, soweit eine E2EE-Verschlüsselung eingesetzt wird (dazu sogleich).

1.2.2.2. Ggf. teilweiser Ausschluss der Anwendbarkeit der DSGVO durch E2EE

Die Anwendbarkeit der DSGVO richtet sich nach den jeweils betroffenen Verarbeitungsvorgängen in der Zielarchitektur.

Sind sämtliche Inhaltsdaten fachverfahrensseitig durchgängig E2EE-verschlüsselt – was dem IT-PLR-Beschluss zur Neukonzeption von OSiP entsprechen würde – und im Transport nur Routing-Metadaten sichtbar, so hat die FITKO (bzw. in ihrem Auftrag der technische IT-Dienstleister) bei der Bereitstellung des Transportdienstes insoweit keinen Zugriff auf personenbezogene Inhaltsdaten im Klartext. Es stellt sich dann die Frage, ob die Daten für die FITKO (bzw. den IT-Dienstleister) überhaupt Personenbezug im Sinne der DSGVO aufweisen und damit die DSGVO anwendbar ist.

Die jüngste Rechtsprechung des EuGH zur Relativität des Personenbezugs spricht stark dafür, dass im Falle einer E2EE die verschlüsselten Daten für die FITKO nicht als personenbezogen anzusehen wären. So hat der EuGH entschieden, dass ein Dienstleister, der pseudonymisierte Daten erhält, aber keinen Zugriff auf die Zuordnungsregel hat, keine personenbezogenen Daten verarbeitet: *„Wie […] ausgeführt, kann die Pseudonymisierung also je nach den Umständen des*

[113] Theoretisch könnte eine Rechtsgrundlage für ein Verarbeitung durch die FITKO geschaffen werden; insbesondere durch einen transformierten Beschluss des IT-PLR oder durch Staatsvertrag.

Einzelfalls andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, so dass letztere für die anderen Personen nicht oder nicht mehr identifizierbar ist."[114]

Dieses Urteil wird weithin als finale Bestätigung der Rechtsauffassung vom „relativen Personenbezug" gelesen. Diese Auffassung war im juristischen Schrifttum schon seit langer Zeit mehrheitlich vertreten – wenngleich auch, insbesondere im Umfeld der Aufsichtsbehörden, bestritten – worden.[115] Sie besagt, dass es für die Bestimmung des Personenbezugs auf die („relative") Perspektive dessen ankommt, der die Daten verarbeitet, und damit darauf, ob eben dieser Verarbeiter die Daten mit dem für ihn zugänglichen Zusatzwissen den betroffenen Personen zuordnen, diese also identifizieren kann. Der EuGH sagt nun letztlich sehr deutlich – am Beispiel von pseudonymisierten Daten – dass der Personenbezug insofern relativ zu bestimmen ist.

An diese Feststellung knüpft sich die bedeutende Rechtsfolge, dass Daten, die nicht personenbezogen sind, anonym sind. Die Verarbeitung anonymer Daten unterliegt nicht dem Anwendungsbereich der DSGVO oder des sonstigen Datenschutzrechts.

Das dem EuGH-Fall zugrunde liegende Beispiel kann ohne Weiteres von pseudonymisierten Daten auf verschlüsselte Daten übertragen werden und bedeutet dann, dass eine Stelle außerhalb des Verantwortlichen, die ausschließlich verschlüsselte Daten erhält, aber keinen Zugriff auf die Schlüssel hat (und sich auch nicht verschaffen kann), keine personenbezogenen Daten verarbeitet.[116] Auch in einer solchen Konstellation sind die Daten nunmehr nach der Rechtsprechung des EuGH anonym.

Auch der – für die FITKO AöR zuständige – hessische Datenschutzbeauftragte hat das EuGH-Urteil in einer Pressemitteilung begrüßt und die Rechtsfolgen der Anonymität und dann nicht mehr gegebenen Anwendbarkeit der DSGVO klargestellt:

> *„Mit diesem überzeugenden Urteil bekräftigt der EuGH seine bisherige Rechtsprechung zur Anonymität von Daten. Es widerlegt eindeutig das bisher vielfach vertretene absolute Verständnis von Anonymität, nach dem die Möglichkeit von irgendjemandem, Daten einer Person zuzuordnen, Anonymität ausschließt. Dadurch wurde der*

---

[114] EuGH, Urt. v. 04.09.2025, Rs. C-413/23 P, Rn. 87.

[115] Vgl. Eckhardt/Rüpke/v. Lewinski, v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3 Aufl., § 10 Rn. 30 m.w.N.

[116] Vgl. Eckhardt/Rüpke/v. Lewinski, v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 3 Aufl., § 10 Rn. 31.

> *Begriff der Anonymität sehr eingeengt und auf sehr seltene Fälle beschränkt. Indem der EuGH der relativen Ansicht von Anonymität folgt, nach der Anonymität immer nur für den jeweiligen Verantwortlichen bestimmt werden muss, wird die Anwendbarkeit der DSGVO auf die praktisch relevanten Fälle beschränkt und Datenverarbeitung – insbesondere für die Entwicklung von KI oder die Durchführung von Forschungsprojekten – erheblich erleichtert."*[117]

Angesichts der zunehmende als geklärt empfunden Rechtslage und zur Befriedigung des lange herrschenden Streits hat die EU-Kommission nunmehr am 19.11.2025 im Rahmen einer unter dem Titel „Digital Omnibus" vorgeschlagenen Novellierung zentraler EU-Gesetze des Datenschutz- und Datenwirtschaftsrechts vorgeschlagen, die Definition der personenbezogenen Daten in Art. 4 Nr. 1 DSGVO wie folgt anzupassen (Anpassung **gefettet**):

> *Art. 4(1) GDPR: For purposes of this Regulation 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;* ***Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.***[118]

Aus Sicht der EU-Kommission handelt es sich dabei ausdrücklich nicht um eine Änderung zur ohnehin geltenden Rechtslage, sondern um eine Klarstellung.[119] Zwar ist diese Klarstellung bisher nur ein Entwurf und damit zeitlich noch weit von ihrer möglichen Verabschiedung entfernt,

---

[117] https://datenschutz.hessen.de/presse/entscheidendes-urteil-des-eugh-zur-anonymitaet-von-daten.

[118] EU Kommission, 2025/0360 (COD), 19.11.2025, S. 54.

[119] EU Kommission, 2025/0360 (COD), 19.11.2025, S. 19.

jedoch ist sie Ausdruck einer weithin empfunden Beendigung des Streits um den Personenbezug im Zuge der zitierten EuGH-Rechtsprechung. Diese Aufnahme in die Definition in der DSGVO würde dann nicht zuletzt IT-Dienstleistern bei der Verarbeitung verschlüsselter Daten (ohne Zugriffsmöglichkeit auf den Schlüssel) letzte Rechtssicherheit geben, dass das Datenschutzrecht auf diese Verarbeitung grundsätzlich nicht Anwendung findet.

Vor diesem Hintergrund sprechen gute Gründe dafür, dass mangels Anwendbarkeit der DSGVO eine Auftragsverarbeitung personenbezogener Inhaltsdaten durch die FITKO nicht vorliegt, soweit die E2EE-Verschlüsselung technisch so umgesetzt ist, dass der FITKO zu keinem Zeitpunkt personenbezogene Daten zugänglich sind (weder Inhalts- noch personenbezogene Metadaten). Unabhängig davon wäre dann allerdings sicherzustellen, dass auch etwaig Telemetrie und Betriebsprotokolle entweder keinen Personenbezug haben oder die Verarbeitung legitimiert wäre.

Es ist jedoch auch bei E2EE davon abzuraten, auf die Vereinbarung einer Auftragsverarbeitung zu verzichten. Dafür sprechen mehrere dringende Gründe:

- So stehen die Folgen der – in dieser Klarheit noch sehr jungen – EuGH-Rechtsprechung aus rechtlicher Sicht noch nicht vollständig fest. Der EuGH hat in dem genannten Urteil zwar den Personenbezug der Daten für den Dienstleister verneint, ist aber gleichwohl aus Sicht des Verantwortlichen von einer Übermittlung ausgegangen, über die die Betroffenen zu informieren seien. Somit ist der Vorgang datenschutzrechtlich nicht von jeglichen Pflichten nach der DSGVO freigestellt. Es ist nicht auszuschließen, dass auch in dieser Konstellation – mit E2EE-verschlüsselten Daten – daher auch eine Auftragsverarbeitung oder zumindest Vereinbarungen mit ähnlicher Schutzwirkung erforderlich sind. Diese könnten zum Beispiel auch für den – theoretischen – Fall erforderlich werden, dass die eingesetzte Verschlüsselung zukünftig nicht mehr wirksam ist, etwa weil sich nicht „quantensicher" ist und leistungsfähige Quantencomputer verfügbar werden. Schon deshalb sollte vorsichthalber eine Auftragsverarbeitung vereinbart werden.
- Dass der Personenbezug für den Dienstleister in der genannten Konstellation fehlt, beruht gerade auf der Tatsache, dass ihm kein (legaler) Zugriff auf die Schlüssel und damit keine Entschlüsselung möglich ist. Schon um dies sicherzustellen, sollten strenge vertragliche Anforderungen an die Aufrechterhaltung dieser Bedingungen gestellt werden. Die Vereinbarung einer Auftragsverarbeitung würde dies mit abdecken und ist daher zu empfehlen.

- Ein Verzicht auf eine Auftragsverarbeitung würde voraussetzen, dass tatsächlich keine personenbezogenen Daten verarbeitet werden. Damit müsste die OSiP-Anwendung also auch außerhalb der E2EE-transportierten Nachrichten keinerlei personenbezogene Daten (z.B. Benutzerdaten, Logfiles) in sichtbarer Form für die FITKO beinhalten. Dies erscheint nach praktischer Erfahrung eher unwahrscheinlich. Sicherheitshalber ist davon auszugehen, dass in Teilen oder Phasen der Verarbeitung doch personenbezogene Daten anfallen können. Sofern die FITKO technisch Zugriff auf die zur Entschlüsselung notwendigen Schlüssel besitzt, liegt bereits eine Verarbeitung vor, unabhängig davon, ob der Zugriff tatsächlich ausgeübt wird. In Fallkonstellationen, in denen die FITKO direkten technischen Zugriff auf den Client erhält (z.B. Remote-Support, Fehlersuche, Telemetrie-Erweiterung), besteht in der Praxis regelmäßig zumindest die Möglichkeit, einzelne Datensätze entschlüsselt einzusehen. Damit ist typischerweise von einer Verarbeitung personenbezogener Daten auszugehen.

Im Ergebnis ist eine E2EE aus Datenschutzsicht unbedingt zu empfehlen. Doch auch wenn sie realisiert ist und auch im Übrigen keine personenbezogenen Daten verarbeitet werde, sollte gleichwohl sicherheitshalber eine Auftragsverarbeitung vereinbart werden, um Datenschutzverstöße (in Form der Verarbeitung ohne Rechtsgrundlage) auszuschließen. Etwas anders gilt nur dann, wenn tatsächlich keine und auch nicht potenziell personenbezogene Daten verarbeitet werden.

1.2.2.3. Verarbeitung im Client (und ggf. im OSiP-Backend)

Wir gehen nach der derzeitigen Planung davon aus, dass mindestens im Client personenbezogenen Daten verarbeitet werden, auf die die FITKO (bzw. der von ihr beauftragte IT-Dienstleister) im Rahmen des Betriebs ggf.. temporär/potenziell Zugriff erhalten kann. Abhängig von dem jeweiligen OSiP-Anwendungsfall werden typischerweise folgende Datenkategorien verarbeitet:

- Identitäts- und Kerndaten der überprüften Person: Name, Vorname, gegebenenfalls Geburtsname, Geburtsdatum und Geburtsort.
- Erkenntnisdaten der Erkenntnisstellen: sicherheitsrelevante Informationen, die von den zuständigen Erkenntnisstellen (z. B. LKA, LfV, BZR, ZStV, GZR) übermittelt werden, etwa Angaben zu Bußgeldern, strafrechtlichen Verurteilungen und Ermittlungsverfahren, sonstigen strafrechtlichen oder ordnungswidrigkeitenrechtlichen Erkenntnissen sowie

Verdachtsfällen. Diese Daten können je nach Inhalt und Herkunft teilweise als „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) eingestuft sein und sind entsprechend den einschlägigen Geheimschutzvorgaben zu behandeln.

- Bewertungs- und Entscheidungsdaten: Ergebnis der Zuverlässigkeitsbeurteilung, also Bejahung oder Verneinung der Zuverlässigkeit sowie Statusänderungen wie Widerruf einer Entscheidung oder Ersuchen.
- Nachberichtsdaten bei nachberichtspflichtigen Stellen: Name, Vorname, Geburtsdatum, Geburtsname, Geschlecht, Geburtsort, Geburtsland, Wohnort und Staatsangehörigkeit. In einzelnen Fachverfahren kommt eine Minimalvariante vor, bestehend aus Name, Vorname, Geburtsort, Geburtsdatum, Wohnort und Staatsangehörigkeit.

Unabhängig von der Frage einer E2EE für ausgetauschte Nachrichten (1.2.2.2.) ist, soweit die genannten Daten ggf. durch die FITKO (bzw. den IT-Dienstleister) im Klartext verarbeitet werden oder ein Zugriff in bestimmten Fällen nicht ausgeschlossen werden kann, eine Auftragsverarbeitung erforderlich.

1.2.3. Nutzung

Bei der Inanspruchnahme des Dienstes verarbeiten die nutzenden Behörden regelmäßig personenbezogene Daten von Antragstellenden, Beschäftigten oder Dritten. Diese Verarbeitung dient der gesetzlichen Aufgabenerfüllung und liegt grundsätzlich in deren eigener Verantwortlichkeit. Zu prüfen bleibt grundsätzlich, ob eine gemeinsame Verantwortlichkeit mit anderen nutzenden Stellen (bei gemeinsamen Verfahren) oder mit der bereitstellenden Stelle vorliegt.

Im Ergebnis ist das Modell einer getrennten Verantwortlichkeit zwischen den nutzenden Stellen zu empfehlen:

- Eine gemeinsame Verantwortlichkeit der nutzenden Stellen untereinander lässt sich auf Basis der einzelnen Rechtsgrundlagen dieser Stellen schwer bis gar nicht begründen, da diese Rechtsgrundlagen jeweils nur die Verarbeitung der Stellen selbst im Rahmen ihrer Aufgaben rechtfertigen. Zudem würde dies den verfassungsrechtlichen Grundsatz der Verantwortungsklarheit berühren. Bei dieser Einschätzung gehen wir davon aus, dass OSiP – gemäß der Zielkonzeption – als gemeinsames IT-Verfahren mit strikter Mandantentrennung konzipiert wird (im Gegensatz etwa zu einer gemeinsamen Datenbank; einem gemeinsame Abrufverfahren etc., für die – soweit ersichtlich – im Fall der ZSÜ keine Rechtsgrundlage besteht).

- Es liegt auch keine gemeinsame Verantwortung zwischen den nutzenden Stellen und der FITKO vor, da es der FITKO insoweit bereits an einer Rechtsgrundlage für eine eigenverantwortliche Verarbeitung von Daten aus einer ZSÜ fehlt (siehe 1.2.1 und 1.2.2).

1.2.4. Rechts- und Rollenfolgen

Wie gesehen sind die nutzenden Behörden (Genehmigungs- und Erkenntnisstellen) Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Die naheliegende datenschutzrechtliche Einordnung der ausgelagerten Verarbeitungsvorgänge ist wie folgt: Die FITKO verarbeitet Daten zur Erbringung des Transport- und ggf. Backoffice-Dienstes als Auftragsverarbeiterin. Das beauftragte Rechenzentrum ist Auftragsverarbeiter bzw. Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

Für den Abschluss der erforderlichen Vereinbarung zur Auftragsverarbeitung kommen dann zwei DSGVO-konforme Umsetzungsvarianten in Betracht:

- **Kettenmodell:** Beim Kettenmodell besteht die Abfolge: Verantwortliche Behörde <–> Auftragsverarbeiter (Anbieter/FITKO) <–> Unterauftragsverarbeiter (Hosting, technischer Betrieb) mit entsprechenden Verträgen nach Art. 28 Abs. 2-4 DSGVO. Hierfür müssen die Datenschutzpflichten in den Verträgen gespiegelt/durchgereicht werden. Es sind klar geregelte Informations- und Genehmigungsprozesse bei Änderungen der Auftragskette sowie vertraglich abgesicherte Audit- und Kontrollrechte gegenüber sämtlichen Beteiligten erforderlich. Weisungen werden entlang der Auftragskette weitergegeben.
- **Sternmodell/Direktmodell:** Beim Direktmodell liegen getrennte Vertragsbeziehungen vor, nämlich verantwortliche Behörde <–> FITKO/Anbieter und verantwortliche Behörde <–> technischer Dienstleister. Es bestehen damit zwei eigenständige Auftragsverarbeitungsverträge mit abgegrenzten Leistungsgegenständen, Weisungswegen, Zuständigkeiten für technische und organisatorische Maßnahmen, festgelegter Datenlokation, definierten Exit- und Reversibilitätsmechanismen sowie abgestimmten Incident-Prozessen. Soweit die FITKO gänzlich aus der Datenverarbeitung ausgenommen ist, kann ggf. im Verhältnis zwischen verantwortlicher Behörde und FITKO auf eine Vereinbarung zur Auftragsverarbeitung verzichtet werden.

Beide Varianten können grundsätzlich datenschutzrechtlich in zulässiger Weise gestaltet werden. Die Entscheidung hat erhebliche Auswirkungen auf Steuerung, Auditpfade, Haftungszuordnung und Eskalationslogik und ist daher im Architektur- und Vertragsdesign ausdrücklich festzulegen.

Vorteilhaft erscheint das Kettenmodell. Wir gehen davon aus, dass dies auch den zivilrechtlichen Vertragsbeziehungen bei Nutzung des FITKO-Produkts „OSiP" entspricht. Ein wesentlicher Vorteil liegt darin, dass die Weisungen in diesem Fall gegenüber der FITKO ergehen und diese daher im Verhältnis zum technischen Dienstleister ihre Steuerungsaufgabe – die auch zu den gewünschten Synergien beiträgt – besser erfüllen kann. Demgegenüber erfordert die Implementierung des Direktmodells eine besonders präzise vertragliche Abgrenzung, um die Einhaltung der Weisungen der Behörde in der gesamten Lieferkette sicherzustellen.

1.3. Mögliche Betriebs- und Verantwortungsmodelle für OSiP

Wie gesehen, ist ein Modell auf Basis der Auftragsverarbeitung datenschutzrechtlich geboten. Ein zentraler Betrieb durch die FITKO mit ausgelagertem technischen Betrieb – gestaltet als Auftragskette – ist angesichts der Planungsziele von OSiP naheliegend und zu empfehlen (1.3.1.). Alternative Modelle werden nachstehend skizziert.

1.3.1. Vorzugsmodell: Zentraler Betrieb durch FITKO; Hosting im Unterauftrag; Praxishinweise zum Vertragsschluss

Die FITKO verfolgt bei allen ihren Angeboten eine einheitlich Produktmanagementstrategie, die sich nach derzeitigem Planungsstand auch für OSiP empfiehlt. Hierbei ist ein zentraler Betrieb durch die FITKO geplant, bei dem das physische Hosting in einem öffentlichen Rechenzentrum oder einem Bundes-/Landeszentrum erfolgt. Die FITKO behält die vollständige Produktsteuerung – sie steuert Weiterentwicklung, Betrieb und Qualitätssicherung – nutzt für den Plattformbetrieb aber eine ausgelagerte Infrastruktur.

Im Vorzugsmodell wird das Hosting als Unterauftragsverarbeitung des Plattformauftrags umgesetzt, das heißt die Behörde schließt einen Auftragsverarbeitungsvertrag mit der FITKO und die FITKO bindet das Rechenzentrum als Unterauftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO ein (Kettenmodell, s. 1.2.4.). Alternativ können die Behörden das Hosting direkt als eigenen Auftragsverarbeitungsvertrag beauftragen und der Plattformbetrieb wird als separater

Auftragsverarbeitungsvertrag parallel geführt (Sternmodell/Direktmodell, s. 1.2.4.). Beide Varianten sind datenschutzrechtlich zulässig, wobei das Kettenmodell vorzugswürdig erscheint (1.2.4.).

Das Kettenmodell erscheint auch praktisch umsetzbar; es kann bei der Entwicklung von Vertragsmodellen und Vorgehensweisen für den Vertragsschluss auf Erfahrungen in anderen Kooperationskontexten zurückgegriffen werden (wie dem Marktplatz für EfA-Leistungen bzw. FIT-Store). Datenschutzrechtlich entscheidend ist, dass im Ergebnis eine (ggf. mehrstufige) datenschutzrechtliche Auftragsbeziehung zwischen jedem Verantwortlichen und dem IT-Dienstleister als (Unter-)Auftragsverarbeiter zustande kommt.[120] Nicht erforderlich ist datenschutzrechtlich eine direkte Beziehung (wie beim Sternmodell). Ebenfalls nicht erforderlich ist datenschutzrechtlich, dass die Verantwortlichen, also die OSiP nutzenden öffentlichen Stellen, beim Abschluss der Vereinbarung zur Auftragsverarbeitung direkt mit dem IT-Dienstleister oder der FITKO kontrahieren.

Der Vertragsschluss der AVV kann sowohl im Ketten- also auch im Sternmodell durch geeignete Vorgehensweisen vereinfacht werden:

- Auftragnehmerseitig ist eine Vereinfachung über ein sog. Beitrittsmodell möglich, wobei der Auftragsverarbeiter einmalig ein AVV-Angebot auf Grundlage eines AVV-Musters an eine Vielzahl von Behörden formuliert. Die Behörden können ihre Annahme dann in Textform erklären.[121]
- Auftraggeberseitig können die Behörden sich beim Abschluss vertreten lassen. Dies ist zum Beispiel auf Ebene des Landes für die Behörden der Landesverwaltung durch das Land oder auf Ebene der Kommunen für deren Behörden durch Kommunalvertreter (z.B. Kommunalverbände) möglich.
- Schließlich können AVV bzw. die zu ihrem Abschluss erforderlichen Erklärungen in den Vertrag bzw. den Vertragsschluss über die Leistungserbringung integriert werden.

Bei den Vertragsmodellen müssen u.a. ggf. vergaberechtliche und landes- und kommunalverfassungsrechtliche Beschränkungen berücksichtigt werden (z.B. durch Inhouse-Modelle). Dies

---

[120] Im Falle der Verarbeitung personenbezogener Daten durch die FITKO oder weitere Dienstleister muss auch eine AVV zwischen den Verantwortlichen und der FITKO und den weiteren Dienstleistern zustande kommen.

[121] Vgl. hierzu FITKO, FAQ – häufig gestellte Fragen rund um den FIT-Store, Stand 20.03.2024, Ziff. 5.2.

ist nur ein Hinweis und nicht Gegenstand dieses Gutachtens. Vertragsmodelle, die (mit den gebotenen Anpassungen für die Anbieterseite) als Blaupause dienen können, sind u.a. im OZG-Kontext entwickelt worden.[122]

1.3.2. Alternative: Zentraler Betrieb durch die FITKO im Eigenbetrieb

Eine Variante des zentralen Betriebs besteht darin, OSiP vollständig in einer von der FITKO kontrollierten Umgebung zu hosten. Rollenbild und Verantwortlichkeiten entsprechen dem Vorzugsmodell, jedoch ohne Unterauftragsvergabe. Der Ansatz bietet theoretisch maximale Steuerbarkeit und kurze Entscheidungswege, geht jedoch mit erheblichem Aufwand zum Aufbau der erforderlichen technischen Kapazitäten und zur Erlangung entsprechender Zertifizierungen einher. Wir gehen davon aus, dass ein solcher eigener technischer Betrieb des Produkts nicht der vorgesehenen Rolle der FITKO entspricht. Er wäre aber datenschutzrechtlich nicht ausgeschlossen (bei Verpflichtung der FITKO als Auftragsverarbeiter).

1.3.3. Alternative: Eigenverantwortlicher Betrieb durch die FITKO

Alternativ kommt ferner prinzipiell ein eigenverantwortlicher Betrieb in Betracht. Jedoch wäre eine Abkehr vom Auftragsverarbeitungsmodell der FITKO für Fachdaten nur dann datenschutzrechtlich zulässig, wenn die gesetzlichen Grundlagen der Fachbehörden dies zulassen oder eine gesetzliche Kompetenznorm für die FITKO besteht. Dies ist derzeit nicht der Fall (1.3.3.1.). Eine Rechtgrundlage müsste also erst geschaffen werden. Dies wäre rechtlich möglich, hätte jedoch keine besonderen Vorteile (1.3.3.2.).

1.3.3.1. Fehlende Rechtsgrundlage für technischen Betrieb (de lege lata)

Der Beschluss des IT-Planungsrats zur OSiP weist der FITKO ausschließlich die Bereitstellung der technischen Infrastruktur zu. Eine eigene fachliche Datenverarbeitung – sei es als alleinige oder als gemeinsame Verantwortliche – ist davon nicht gedeckt. Für staatliche Datenverarbeitungen gilt der Vorbehalt des Gesetzes in seiner Ausprägung als Wesentlichkeitstheorie: Je intensiver der Grundrechtseingriff, desto klarer, bestimmter und begrenzender muss die gesetzliche

[122] Vgl. FITKO, EfA-Nachnutzung und Nachnutzungsmodelle – Eine Übersicht, Stand 27.04.2022; siehe auch den OZG-Hub unter https://www.ozg-hub.de/was-ist-der-ozg-hub/nachnutzung-modelle.

Grundlage die Zwecke, Voraussetzungen, Datenarten, Nutzungen, Speicherdauern und Kontrollmechanismen regeln.[123] Eine bloß generische Ermächtigung „zur Bereitstellung der Infrastruktur" im Beschluss genügt nicht, um eine Verantwortlichkeit oder eine gemeinsame Verantwortlichkeit für die FITKO für Inhaltsdaten zu begründen.

Unberührt bleibt, dass die FITKO ggf. in eng begrenztem Umfang betriebliche personenbezogene Daten verarbeiten kann – etwa Transport-/Routing-Metadaten, Sicherheits- und Protokolldaten oder Störungs-/Incident-Informationen. Diese Verarbeitungen dienen ausschließlich Betrieb, Sicherheit und Nachweis der OSiP-Infrastruktur. Soweit hierfür keine Auftragsverarbeitung gegenüber den fachlich verantwortlichen Behörden vorliegt, kommt getrennte Verantwortlichkeit der FITKO nur für diese eng umschriebenen Betriebszwecke in Betracht. Rechtsgrundlage ist dann regelmäßig Art. 6 Abs. 1 lit. e DSGVO i.V.m. der für die FITKO geltenden landesdatenschutzrechtlichen Generalnorm i.V.m dem öffentlich-rechtlichen Auftrag zur Infrastrukturbereitstellung und den Anforderungen aus Art. 5, 24, 32 DSGVO. Zwingend sind eine strikte funktionale und technische Trennung von Fach- und Betriebsdaten, separate Schlüssel-/Rollenmodelle, minimale Retentionszeiten mit dokumentierten Löschfristen, ein Zweckbindungs- und Zweckänderungs-Check (Art. 6 Abs. 4 DSGVO) sowie transparente Information gegenüber den Behörden. Eine gemeinsame Verantwortlichkeit wird hierdurch nicht begründet; die FITKO bleibt für diese Betriebsverarbeitungen – soweit nicht Auftragsverarbeitung – isoliert verantwortlich.

1.3.3.2. Mögliche Schaffung einer Rechtsgrundlage

Die derzeit fehlende Rechtsgrundlage für die FITKO könnte – jedenfalls theoretisch – geschaffen werden. Hierzu könnten der Bund und die Länder etwa der FITKO per Staatsvertrag entsprechende Aufgaben zur eigenverantwortlichen Erfüllung übertragen.

Ein Beispiel hierfür wäre die GÜL AöR: Die Gemeinsame elektronische Überwachungsstelle der Länder ist eine durch Staatsvertrag errichtete AöR (Art. 1 GÜL-StV). Die Länder haben ihr Aufgaben im Zusammenhang mit der elektronischen Überwachung des Aufenthaltsorts von Personen unter Führungsaufsicht („elektronische Fußfessel") übertragen (Art. 2 GÜL-StV). Der

---

[123] Vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a. („Volkszählungsurteil"), BVerfGE 65, 1, Leitsatz 2: „Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß." Ferner BVerfGE 65, 1 (44 f.) zur Verhältnismäßigkeit sowie (67–70) zu bereichsspezifischer Zweckbestimmung und zusätzlichen organisatorisch-verfahrensrechtlichen Sicherungen bei Datenverarbeitung.

Staatsvertrag enthält auch explizit Rechtsgrundlagen für die Datenverarbeitung durch die GÜL im Rahmen der ihr übertragenen Aufgaben (Art. 3 GÜL-StV). Hieraus ergibt sich – nicht ausdrücklich, aber eindeutig – ihre entsprechende datenschutzrechtliche Verantwortlichkeit.

In vergleichbarer Weise könnte – theoretisch – auch die FITKO AöR eigenverantwortlich mit dem Betrieb von OSiP beauftragt werden. Ob dies bereits – bei hinreichend spezifischer Ausgestaltung der Rechtsgrundlage – auf Basis des jetzigen IT-StV möglich ist (durch verbindliche Beschlüsse des IT-PLR) oder eines weiteren bzw. geänderten Staatsvertrags bedürfte und inwieweit die Aufgabenübertragung zulässig wäre, müsste verfassungsrechtlich noch geprüft werden.

Ein solches Vorgehen hätte jedoch keine erheblichen Vorteile gegenüber der klaren und etablierten Betriebsform der Auftragsverarbeitung. Zudem würde das Schaffen einer Rechtsgrundlage einen erhöhten Abstimmungsaufwand erfordern und Verzögerungen gegenüber dem bereits jetzt möglichen und gängigen Verfahren der Auftragsverarbeitung bedeuten. Rein aus Datenschutzsicht spricht daher wenig dafür, den Aufwand für die Schaffung einer Rechtsgrundlage zu betreiben.

1.3.4. OSiP als reiner Transportdienst; Fachverfahren dezentral in den Ländern

Dies entspricht dem bisherigen Status: Die FITKO stellt eine abgesicherte Transport- und Validierungsschicht bereit. Der technische Betrieb der Backoffice-Module und Erkenntnis-Clients verbleibt in der Verantwortung der Länder. Die Behörden bleiben Verantwortliche. Die FITKO ist Auftragsverarbeiterin für den Transport.

Rein datenschutzrechtlich ist dieser Ansatz möglich. Er betont die Länderautonomie, begrenzt aber die Harmonisierung des Verfahrens und erreicht nicht die gewünschten Ziele eines vereinfachten IT-Betriebs mit entsprechenden Effizienzsteigerungen.

1.3.5. Empfehlung

Empfohlen wird der zentral verantwortete Betrieb der gesamten OSiP-Infrastruktur durch die FITKO mit ausgelagertem Hosting im Unterauftrag (1.3.1.). Die nutzenden Stellen bleiben dabei (getrennt) Verantwortliche. Die technische Verarbeitung durch die FITKO ist strikt im Auftragsverarbeitungsmodell zu führen und durch klare Verträge, angemessene TOMs und eine saubere Unterauftragskette abzusichern. Datenschutzrechtlich zu empfehlen – wenn nicht sogar unter dem Aspekt der technisch-organisatorischen Sicherheit geboten (siehe 4.) – bleibt die durchgängige Ende-zu-Ende-Verschlüsselung, damit die FITKO keine Inhaltsdaten im Klartext

verarbeitet. Auch in diesem Fall – selbst wenn ansonsten keine personenbezogenen Daten verarbeitet würden – ist aber der Abschluss einer AVV oder jedenfalls von weitgehend entsprechenden Regelungen zu empfehlen (1.2.2.2.). Nur in den Fällen, in denen eindeutig und dauerhaft keine Verarbeitung personenbezogener Daten erfolgt – also auch keine personenbeziehbaren Meta- oder Logdaten anfallen –, kann darauf verzichtet werden.

1.4. Folgen: Umsetzung datenschutzrechtlicher Anforderungen

1.4.1. Datenschutzschutzorganisation und -grundsätze

Nach dem empfohlenen Betriebsmodell sind die Verantwortlichen und die FITKO als Auftragsverarbeiterin an die Grundpflichten der DSGVO gebunden. Maßgeblich ist insbesondere die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO), die durch die folgenden Dokumente und Prozesse zu gewährleisten ist:

- Verarbeitungsverzeichnisse (VVT): Die fachlich verantwortlichen Behörden (Art. 30 Abs. 1 DSGVO) und die FITKO bzw. der technische Dienstleister als (Unter-)Auftragsverarbeiterin (Art. 30 Abs. 2 DSGVO) führen separate, die technische Zielarchitektur abbildende Verzeichnisse. Zwingend abzubilden sind insbesondere Datenkategorien, Empfängergruppen, TOMs sowie etwaige gemeinsame Verantwortlichkeiten und Auftragsketten.
- Technische und Organisatorische Maßnahmen (TOM): Die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme nach Art. 32 DSGVO ist durch dokumentierte TOMs sicherzustellen (siehe 4.1.).
- Informationssicherheits- und Compliance: Die Sicherheitsorganisation ist an BSI-Standards/IT-Grundschutz auszurichten und der IT-Dienstleister muss voraussichtlich die kommenden KRITIS/NIS2-Regeln implementieren (4.2.). Das Risikomanagement muss u.a. Lieferkettenrisiken und ein regelmäßiges Audit- und Berichtswesen umfassen. Für Verschlusssachen (VS-NfD) sind die Vorgaben des Geheimschutzes zu berücksichtigen (I.1.3.).
- Privacy by Design and by Default (Art. 25 DSGVO): Bereits im Entwurf sind die Grundsätze der Datenminimierung, strikten Trennung von Fach- und Betriebsdaten, nach Möglichkeit durchgängigen Verschlüsselung (E2EE) und ggf. der Einsatz von Pseudonymisierung zu prüfen und umzusetzen.

- Datenschutz-Folgenabschätzung (DSFA, Art. 35 DSGVO): Eine DSFA ist durchzuführen (2.).
- Übermittlungen und Datenlokation: Die Datenlokation ist verbindlich festzulegen. Im Ergebnis sollte die Verarbeitung in Deutschland stattfinden.
    - Kapitel V DSGVO: Rein datenschutzrechtlich sind Drittlandübermittlungen im Prinzip möglich (siehe aber den nächsten Spiegelstrich), wenn die Anforderungen der Art. 44 ff. DSGVO erfüllt und abgesichert werden (einschließlich Transfermechanismus und Transfer-Impact-Assessments). Aufgrund der Sensibilität der Daten und der besonderen Sicherheitsanforderungen ist jedoch – schon aus Datenschutzsicht – eine Verarbeitung in der EU und idealerweise in Deutschland zu empfehlen, um Kontrollmöglichkeiten sicherzustellen und Risiken zu minimieren.
    - Nationale digitale Souveränität: Unter Berücksichtigung der Netzstrategie 2030 sollte als Standort der Verarbeitung Deutschland gewählt werden. Dies entspricht dem darin formulierten Ziel der „nationalen digitalen Souveränität". Bereits die „Gesamtstrategie IT-Netze der öffentlichen Verwaltung" (2013) hat das Leitbild formuliert, dass der Bund kritische IT-Systeme und Infrastrukturen soweit wie möglich selbst plant, aufbaut und betreibt oder zumindest die Kontrolle darüber hat.[124] In der Netzstrategie 2030 ist dies als „nationale digitale Souveränität" formuliert: „*Die öffentliche Verwaltung verfolgt für den IVÖV ein Eigenbetriebsmodell durch einen internen Netzerdienstleister … Dies umfasst auch Beschaffung von Produkten und Dienstleistungen sowie Vorgaben zur Übertragung von Daten ausschließlich innerhalb deutscher Landesgrenzen (nationales Routing).*"[125] Zwar ist die Netzstrategie 2030 als Strategiepapier des Bundes nicht unmittelbar bindend. Sie ist aber vom IT-Rat des Bundes im Februar 2019 beschlossen worden und insofern auf Bundesebene eine verbindliche Vorgabe. Im föderalen Kontext hat der IT-PLR die Netzstrategie in einem Beschluss zur

[124] Zitiert nach CIO Bund, Netzstrategie 2030 für die öffentliche Verwaltung, November 2018, S. 3.

[125] CIO Bund, Netzstrategie 2030 für die öffentliche Verwaltung, November 2018, S. 9.

Kenntnis genommen.[126] Sie ist daher bei der Planung von IT-Produkten zu berücksichtigen. Danach sollte zumindest sinngemäß an OSiP als besonders sicherheitssensibles Produkt nach Möglichkeit die beschriebenen Anforderungen gestellt werden (nationales Routing; Betrieb innerhalb deutscher Landesgrenzen).

- Verbundnetz: Schließlich muss der Datenaustausch nach den Vorgaben des IT-NetzG über das Verbundnetz erfolgen, sodass der Betreiber (FITKO bzw. der technische Dienstleister) an dieses anzuschließen ist und die Anschlussbedingungen einhalten muss (siehe I.1.2.3.2 und III.1.1). Auch dies spricht dafür, dass das anzubindende Netzsegment des Betreibers in Deutschland liegen sollte.

1.4.2. Auftragsverarbeitung

Da die FITKO (und der technische IT-Dienstleister) als Auftragsverarbeiterin tätig wird, ist die Zusammenarbeit vertraglich abzusichern. Hierbei obliegen der OSiP nutzenden Behörde als datenschutzrechtlich verantwortlicher Stelle umfangreiche Kontroll- und Überwachungspflichten.

- Prüfung des Auftragnehmers (Art. 28 Abs. 1 DSGVO): Der Auftragnehmer (und Unterauftragnehmer) muss durch Datenschutz- und Sicherheitskonzepte sowie geeignete Zertifizierungen hinreichend Gewähr bieten für die Einhaltung der datenschutzrechtlichen Anforderungen.
- Auftragsverarbeitungsvertrag (Art. 28 Abs. 3 DSGVO): Er muss Gegenstand, Dauer, Art, Zweck und Datenkategorien regeln. Das Weisungsmodell ist eindeutig zu regeln (inkl. Dokumentations- und Eskalationswege).
- Unterauftragsverarbeitung: Die Einbindung des Rechenzentrums als Unterauftragnehmer bedarf der Genehmigung des Verantwortlichen (Art. 28 Abs. 2 DSGVO). Die Pflichten des Unterauftragnehmers müssen mit denen der FITKO aus der Haupt-Vereinbarung korrespondieren (Art. 28 Abs. 4 DSGVO).
- TOMs, Datenlokation, Exitstrategie: Die TOMs müssen vertraglich die technische Zielarchitektur widerspiegeln, die Datenlokation festschreiben und Exitszenarien vorsehen

[126] IT-PLR, Beschluss 2018/42 (27. Sitzung) vom 25.10.2018.

(geordnete Rückgabe/Löschung von Daten, Konfigurationen, Schlüsseln). SLAs/OLAs müssen datenschutzrelevante Metriken enthalten.

- Incident- und Breach-Prozesse (Art. 33, 34 DSGVO): Abgestimmte Prozesse zur unverzüglichen Information und Unterstützung des Verantwortlichen bei Sicherheitsvorfällen und meldepflichtigen Verletzungen sind zwingend vorzuhalten. Es ist ein übergreifender Breach-Prozess zu etablieren, der die Anforderungen des Datenschutzes und der IT-Sicherheit (einschließlich KRITIS/NIS2-VO) umsetzt.
- Mandantentrennung: Eine strikte Mandantentrennung ist durch angemessene Maßnahmen zur physischen, jedenfalls aber zur sicheren logischen Trennung umzusetzen.
- Strikte Trennung von Fach- und Betriebsdaten: Funktionale und organisatorische Trennung von Betriebs- und Telemetriedaten von den Fachdaten ist mittels getrennter Datenflüsse, Speicherbereiche, Rollen- und Schlüsselmodelle sowie differenzierten Löschkonzepten sicherzustellen.
- Unterstützungs- und Nachweispflichten: Die FITKO bzw. der technische Dienstleister muss die Verantwortlichen umfassend unterstützen (Betroffenenrechte, Sicherheit, Meldungen, DSFA, Audits) und sämtliche zum Nachweis der Einhaltung (Art. 28 DSGVO) erforderlichen Informationen bereitstellen.

2. DSFA-Pflichten

Frage: *„Wer ist zur Durchführung der DSFA verpflichtet? Kann eine zentrale DSFA für die Plattform erstellt werden oder müssen die einzelnen Länder jeweils eigene durchführen?"*

Kurzantwort:

Die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) ist für OSiP zwingend erforderlich, da die umfangreiche Verarbeitung von sensiblen Daten (ggf. Art. 9 und insb. Art. 10 DSGVO) und die mögliche Verkettung von Daten aus unterschiedlichen Quellen ein hohes Risiko indiziert.

Die FITKO ist als Auftragsverarbeiterin nicht selbst verpflichtet, eine DSFA durchzuführen, hat die Verantwortlichen aber umfassend zu unterstützen. Aufgrund der zentralisierten Architektur und der föderalen Struktur ist das Vorgehen zweistufig zu gestalten:

1. Zentrale Muster-DSFA: Die FITKO sollte eine Muster-DSFA für die Nutzung der OSiP-Plattform unter Berücksichtigung aller absehbaren Risiken erstellen.
2. Behördenspezifische Ergänzungen: Soweit es bei den nutzenden Fachbehörden (als Verantwortliche) Abweichungen oder Ergänzungen gibt (z.B. Löschfristen, Workflows) ist eine landesspezifische Ergänzung auszufüllen und das fachliche Restrisiko zu dokumentieren.

Vorabkonsultation (Art. 36 DSGVO): Sollte ein hohes Restrisiko verbleiben (was durch die technischen-organisatorischen Maßnahmen der Zielarchitektur regelmäßig vermieden werden sollte), müsste die Konsultation dezentral durch die jeweiligen Fachbehörden bei ihrer zuständigen Aufsichtsbehörde erfolgen.

2.1. Zuständigkeit für die Durchführung der DSFA (Art. 35 DSGVO)

Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) trifft den Verantwortlichen. Nach Art. 35 Abs. 1 DSGVO hat der Verantwortliche vor Beginn der Verarbeitung eine DSFA durchzuführen. Eine einzige DSFA kann eine Reihe ähnlicher Verarbeitungsvorgänge mit ähnlichen Risiken abdecken (Art. 35 Abs. 1 S. 2 DSGVO).

Nach dem Vorzugsmodell ist von einer getrennten Verantwortlichkeit der jeweils nutzenden Fachbehörde auszugehen: Die jeweils nutzende Fachbehörde ist Verantwortliche der fachverfahrensbezogenen Nutzung und daher DSFA-pflichtig, sofern die Tatbestandsmerkmale erfüllt

sind. Auftragsverarbeiter (hier: FITKO) sind nicht eigenständig DSFA-pflichtig, müssen den Verantwortlichen aber bei den Pflichten nach Art. 32 bis 36 DSGVO unterstützen (Art. 28 Abs. 3 Buchst. f DSGVO).

2.2. Erforderlichkeit einer DSFA für OSiP

2.2.1. Stufe 1: Prüfung nach Art. 35 Abs. 3 DSGVO (Regelbeispiele)

Art. 35 Abs. 3 DSGVO enthält Regelbeispiele, in denen stets eine DSFA durchzuführen ist.

Nicht einschlägig ist das Regelbeispiel der Entscheidung mit Rechtswirkung aufgrund einer systematischen und umfassenden Bewertung persönlicher Aspekte (Art. 35 Abs. 3 Buchst. a DSGVO), da OSiP selbst keine automatisierten Entscheidungen trifft. Ebenso nicht einschlägig ist das Regelbeispiel einer systematischen, umfangreichen Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 Buchst. c DSGVO).

Demgegenüber ist das Regelbeispiel der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von Daten nach Art. 10 DSGVO (Art. 35 Abs. 3 Buchst. b i.V.m. Art. 9, 10 DSGVO) im Kontext sicherheits- bzw. zuverlässigkeitsrechtlicher Prüfungen wohl erfüllt. Dies gilt jedenfalls bezogen auf das Gesamtsystem, aber je nach verantwortlicher Stelle bei entsprechend häufiger Nutzung auch bei isolierter Betrachtung aus Sicht der Stelle.

Bereits die Erfüllung eines Regelbeispiels führt zur Pflicht, eine DSFA durchzuführen. Da bei der gebotenen vorsichtigen Betrachtung ein Regelbeispiel erfüllt sein dürfte, ist daher eine DSFA erforderlich.

2.2.2. Stufe 2: Positivlisten der Aufsichtsbehörden (Art. 35 Abs. 4 DSGVO)

Für öffentliche Stellen existieren „Positivlisten“ von Verarbeitungen, bei denen zwingend eine DSFA durchzuführen ist. Der BfDI (Bund) führt eine bundesweite Liste für Bundesbehörden. Mehrere Länder (z.B. NRW, Hamburg) führen eigene Positivlisten. Eine explizite Nennung von „OSiP“ bzw. von ZSÜ findet sich in keiner der Listen. Nach Gegenstand und Eingriffsintensität können OSiP-Verarbeitungen jedoch ggf. unter die dortige Fallgruppen fallen, nämlich insbesondere unter umfangreiche Verarbeitung von Daten nach Art. 9 DSGVO bzw. Art. 10 DSGVO. Auch dies spricht schon aus Gründen der Vorsicht für die Durchführung einer DSFA.

2.2.3. Stufe 3: Risikoeinschätzung nach Art. 35 Abs. 1 DSGVO (EDPB-Kriterien)

Nach den EDPB-Leitlinien zur DSFA (WP248 rev.01) ist eine DSFA in der Regel erforderlich, wenn zwei oder mehr der dort definierten Risikokriterien vorliegen. In diesem Fall ist regelmäßig voraussichtlich von einem hohen Risiko auszugehen. Für OSiP sind – je nach Implementierung – regelmäßig die folgenden Indikatoren einschlägig oder es liegt zumindest eine vergleichbare risikogeneigte Verarbeitung vor:

- Bewertung/Einstufung persönlicher Aspekte im Rahmen von ZSÜ;
- Verarbeitung sensibler oder „hochpersönlicher" Daten, darunter besondere Kategorien nach Art. 9 DSGVO und Daten nach Art. 10 (strafrechtliche Bezüge);
- großes Ausmaß durch wiederkehrende, föderal verbreitete Verfahren mit potenziell hoher Betroffenenzahl;
- Zusammenführung von Informationen aus verschiedenen Quellen (mehrere Erkenntnisstellen/Registerschnittstellen, wenn auch ohne unzulässige automatisierte Abgleiche;
- schutzbedürftige Betroffenengruppen wie Bewerbende/Beschäftigte in Abhängigkeitsverhältnissen;
- erhebliche Auswirkungen der behördlichen Entscheidung auf die berufliche Tätigkeit der Betroffenen.

Schon zwei dieser Indikatoren können eine DSFA auslösen; bei mehreren ist regelmäßig von einem hohen Risiko auszugehen.

2.2.4. Zwischenergebnis

Für OSiP besteht eine Pflicht zur Durchführung einer DSFA. Verantwortlich sind die jeweils nutzenden Fachbehörden als Verantwortliche. Die FITKO ist Auftragsverarbeiterin und unterstützt nach Art. 28 Abs. 3 Buchst. f DSGVO.

2.3. Zentrale DSFA, Muster-DSFA bzw. Baustein-DSFA für OSiP

Eine zentrale, produktbezogene DSFA für OSiP ist rechtlich zulässig, wenn sie tatsächlich ähnliche Verarbeitungsvorgänge mit vergleichbaren Risiken beschreibt. Der Wortlaut von Art. 35 Abs. 1 Satz 2 DSGVO erlaubt eine einzige DSFA für ähnliche Vorgänge. Die Aufsichtspraxis und der EDSA erkennen zudem an, dass Verantwortliche sich auf eine bestehende DSFA stützen

dürfen, sofern diese die eigene Implementierung hinreichend abdeckt, und dass mehrere Verantwortliche eine gemeinsame DSFA für ein Gruppen- oder Plattformprojekt durchführen können.[127] Die Zulässigkeit einer Muster-DSFA ist für OSiP besonders gegeben, da es sich um ein zentral entwickeltes und föderal harmonisiertes Produkt handelt, dessen Kernarchitektur und die zugrundeliegenden Risikofaktoren in allen Ländern gleich sind. Bei Abweichungen ist eine ergänzende behördenspezifische Bewertung erforderlich. Entscheidend bleibt stets die Deckungsgleichheit der Risiken und Maßnahmen. Weichen Umsetzung oder Risiken ab, ist eine behördenspezifische Ergänzung erforderlich.

Neben dem Ansatz der „zentralen DSFA" kann eine zentrale von der FITKO bereitgestellte Risikoanalyse auch ein Baustein für die von der jeweiligen Behörde durchzuführende DSFA angesehen werden. Dies entspricht dem Vorgehen der „verteilten Risikoanalyse". Bei diesem Vorgehen wird die Erstellung von Risikoanalysen (bzw. DSFA) für bestimmte Bausteine eines Verfahrens – wie das Betriebsmittel OSiP – separat durchgeführt und von den nutzenden Behörden in die von ihnen durchzuführende DSFA integriert. Dies entspricht den Empfehlungen der Aufsichtsbehörden für Verarbeitungstätigkeiten, bei denen in einem engen fachlichen Sachzusammenhang mehrere Stellen zusammenwirken, wie das bei der zentralen Bereitstellung von IT-Anwendungen der Fall ist.[128]

2.4. Empfohlenes Vorgehensmodell für OSiP

Als Anbieter von OSiP ist die FITKO ohnehin verantwortlich, OSiP umfassend zu dokumentieren und eine Risikoanalyse durchzuführen (wenngleich keine DSFA im Sinne von Art. 35 DSGVO, da keine datenschutzrechtliche Verantwortlichkeit für die Inhaltsdaten besteht). Für die OSiP-Zielarchitektur empfiehlt sich daher ein zweistufiges Vorgehen: Erstens sollte die FITKO eine zentral koordinierte „Muster-DSFA" (bzw. Baustein-DSFA) für OSiP verfassen (Architektur, Mandantentrennung, Rollen- und Berechtigungsmodell, Protokollierung, Löschung/Aufbewahrung, Administrations- und Supportprozesse), die die gleichartigen technischen Risiken und Standard-Abhilfemaßnahmen dokumentiert. Dieses Muster bzw. dieser Baustein sollte den nutzenden Behörden zur Verfügung gestellt und von diesen ggf. adaptiert und eigenverantwortlich übernommen werden. Die Risikoanalyse bzw. Muster-DSFA sollte mit ausreichendem Vorlauf

[127] Vgl. DSK, WP248 rev.01, S. 8.

[128] Vgl. BayLfD, Risikoanalyse und Datenschutz-Folgenabschätzung, V1.0, 1. Mai 2022, S. 60 ff. und S. 71.

vor Aufnahme eines Pilot- oder Echtbetriebs von OSiP vorliegen, damit bei Bedarf DSFA-Ergebnisse (im Sinne von noch erforderlichen Maßnahmen) noch umgesetzt werden bzw. in die Systemgestaltung einfließen können und damit die verantwortlichen Behörden ihrerseits genug Zeit zur Prüfung und Vorbereitung der eigenen Dokumentation haben.

Sollten sich Abweichungen bei Risiken oder Umsetzung ergeben, dokumentiert die jeweilige Stelle diese in den gebotenen behördenspezifischen Ergänzungen. Verbleibt trotz Maßnahmen ein hohes Restrisiko, ist die Vorabkonsultation nach Art. 36 DSGVO durch die jeweils zuständige Behörde einzuleiten. Da die Aufsichtsbehörden der Länder für ihre jeweiligen Landesbehörden zuständig sind, muss die Muster-DSFA der FITKO zwar die Konsultation vorbereiten, die Vorabkonsultation nach Art. 36 DSGVO bei verbleibendem hohem Restrisiko muss aber durch die jeweilige Fachbehörde bei der für sie zuständigen Landesdatenschutzaufsichtsbehörde (oder für Bundesbehörden beim BfDI) erfolgen. Eine zentrale Konsultation für alle Länder durch die FITKO ist aufgrund der fachlich getrennten Verantwortlichkeiten und aufsichtsbehördlichen Zuständigkeiten nicht möglich. Ggf. findet aber intern seitens der DSK eine Koordinierung der Prüfung statt.

Sollte eine Konstellation gemeinsamer Verantwortlichkeit vorliegen – wie gezeigt hier eher fernliegend –, sollte die Vereinbarung nach Art. 26 DSGVO „klar und transparent" festlegen, wer welche DSGVO-Pflichten wahrnimmt, also auch, wer für die Durchführung der DSFA zuständig sein soll.

3. Alternative Betriebsmodelle zur Zielarchitektur

Frage: *„Welches Betriebsmodell müsste ggf. alternativ gewählt werden?"*

Kurzantwort:

Das in der Zielarchitektur angestrebte Betriebsmodell (zentraler Betrieb durch die FITKO bzw. in ihrem Auftrag durch den technischen IT-Dienstleister) ist datenschutzrechtlich umsetzbar. Nach der bestehenden Rechtslage ist die FITKO dabei als Auftragsverarbeiter zu verpflichten und zu empfehlen der IT-Dienstleister sollte als Unterauftragsverarbeiter verpflichtet werden (Kettenmodell).

Mithin ist es aus Datenschutzsicht nicht erforderlich, ein alternatives Betriebsmodell zu wählen. Sollte das empfohlene zentrale Auftragsverarbeitungsmodell in Form des Kettenmodells (oder des Direktmodells) aus anderen Gründen nicht möglich oder nicht gewünscht sein, kommen folgende Alternativen in Betracht.

Alternativmodell	Kurzbeschreibung	Bewertung
FITKO-Eigenbetrieb	Die FITKO betreibt OSiP vollständig in eigener Infrastruktur (ohne Unterauftragnehmer).	Bietet maximale Steuerbarkeit und kurze Entscheidungswege. Erfordert jedoch hohe Investitionen und den vollen Nachweis der Betriebsreife bei der FITKO. Wir gehen nicht davon aus, dass dies der Aufgabenstellung der FITKO entspricht und in Betracht kommt.
Dezentraler Eigenbetrieb	Status quo. Jedes Land betreibt seine OSiP-Instanz alleinverantwortlich (bei einem öffentlichen IT-Dienstleister als Auftragsverarbeiter).	Datenschutzrechtlich zulässig, aber mit Blick auf die im Rahmen der IT-Kooperation über den IT-PLR allgemein strategisch verfolgten Ziele und auch die konkret mit OSiP verfolgten Planungsziele nicht zu empfehlen. Wahrt maximale Autonomie, ist aber ineffizient und widerspricht dem Harmonisierungsziel des IT-PLR (Beschlusslage). Geringere Nutzung von Synergien, erhöhter Wartungs- und Pflegeaufwand. Im Zweifel schwierigere Standardisierung und höhere Komplexität bei Implementierung des angestrebten E2EE-Verfahrens.

Landes- oder Verbund-betrieb	Ein Land oder Landesrechenzentrum übernimmt den zentralen Betrieb als Shared Service für andere Länder.	Datenschutzrechtlich möglich. Erfordert zwischenstaatliche Verwaltungsvereinbarungen und präzise AV-Verträge zwischen allen nutzenden Ländern/Stellen und dem Betreiberland bzw. betreibenden IT-Dienstleister.
Gemeinsame Verantwortlichkeit (Art. 26 DSGVO)	FITKO und Länder legen Zwecke/Mittel der Verarbeitung gemeinsam fest.	Fernliegend und nicht empfehlenswert. Mangels spezifischer Rechtsgrundlage für die FITKO ist dieses Modell für die Verarbeitung von Inhaltsdaten unzulässig (Verstoß gegen die Wesentlichkeitstheorie).

Sofern das empfohlene Vorzugsmodell – ein durch die FITKO zentral gesteuerter Betrieb als Auftragsverarbeiterin mit ausgelagertem Hosting (siehe 1.) – nicht umgesetzt werden kann oder soll, kommen die nachfolgend dargestellten Konstellationen in Betracht.

Maßgeblich für die Zulässigkeit jedes Alternativmodells bleibt die klare Trennung von Fach- und Betriebsdaten sowie die eindeutige Zuweisung der datenschutzrechtlichen Rollen nach Art. 4 Nr. 7, Art. 26 und Art. 28 DSGVO. Die Wahl der Alternative hängt primär vom gewünschten Grad der föderalen Autonomie und dem akzeptierten Betriebsrisiko ab.

3.1. FITKO-Eigenbetrieb ohne Unterauftragsverarbeiter

Die FITKO betreibt OSiP vollständig in einer von ihr kontrollierten Infrastruktur. Die fachlich entscheidenden Behörden bleiben Verantwortliche. Die FITKO verarbeitet Fachdaten als Auftragsverarbeiterin. Betriebs- und Sicherheitsdaten können in eng begrenztem Umfang in eigener, strikt getrennt zu dokumentierender Verantwortlichkeit verarbeitet werden. Das Modell bietet maximale Steuerbarkeit, kurze Entscheidungswege und eine einheitliche Sicherheitslinie. Es erfordert zugleich einen erhöhten Nachweis- und Betriebsaufwand.

Wesentliche Anforderungen: Ein umfassender Auftragsverarbeitungsvertrag zwischen Behörde und FITKO, ein vollständiges TOM-Konzept, klare Weisungs- und Eskalationswege, Exit- und Reversibilitätsmechanismen sowie ein dokumentiertes Audit- und Berichtswesen. Erforderlich sind zudem ein durchgängiges ISMS nach BSI-Standards, die Fähigkeit zum 24/7-Betrieb einschließlich gelebter Notfall- und Wiederanlaufverfahren sowie belastbare Zertifizierungen und regelmäßige Audits.

Einschätzung: Datenschutzrechtlich wohl zulässig, wobei der Eigenbetrieb nach unserem Verständnis nicht der vorgesehen Aufgabe der FITKO entspricht. Vorteil wäre eine hohe Vereinheitlichung und Steuerbarkeit. Allerdings ergibt sich für die FITKO eine Konzentration von Betriebsrisiken und ein erheblicher Investitionsbedarf zur Erlangung der eigenen Betriebsreife.

3.2. Dezentraler Eigenbetrieb

Dieses Modell entspricht im Wesentlichen dem aktuellen Ist-Zustand. Jedes Land betreibt seine OSiP-Instanz eigenständig und bleibt alleinige Verantwortliche für die fachliche Verarbeitung. Die FITKO agiert primär als zentraler Softwareentwickler, Produktmanager und Lizenzgeber. Der Ansatz schützt föderale Besonderheiten und bestehende Betriebsstrukturen. Er erschwert jedoch die länderübergreifende Harmonisierung, verlängert Release-Zyklen und erhöht den Koordinationsaufwand. Eine durchgängige Ende-zu-Ende-Verschlüsselung mit einheitlicher Schlüsselhoheit ist länderweit nur mit erheblichem Abstimmungsaufwand erreichbar.

Wesentliche Anforderungen:

- Je Land ein eigener Auftragsverarbeitungsvertrag mit dem Landes- oder Bundesrechenzentrum, einschließlich eindeutiger Weisungswege, TOM, Datenlokation, Exit-Szenarien und Incident-Prozessen.
- Einheitliche Mindeststandards für Schnittstellen, Protokollierung, Schlüssel- und Rollenmodelle sowie Lösch- und Aufbewahrungskonzepte, um Interoperabilität sicherzustellen.
- Ein zentrales Produkt- und Release-Management der FITKO mit verbindlichen Mindestanforderungen, Regressionstests und Abnahmeprozessen, damit länderspezifische Anpassungen nicht zu Fragmentierung führen.
- Ein abgestimmtes Sicherheits- und Compliance-Rahmenwerk mit regelmäßigen Audits, Benchmarking der TOM und einem föderalen Koordinationsgremium für Änderungen, Sicherheitsvorfälle und Patches.

Einschätzung: Datenschutzrechtlich zulässig. Aus Sicht der Länder ergibt sich eine hohe Autonomie und Anschlussfähigkeit an Landesprozesse. Jedoch werden die auf föderaler Ebene vom IT-PLR vorgegebenen Planungsziele nicht erreicht: Effizienz- und Skalennachteile, komplexe Koordination, erhöhte Angriffsfläche durch heterogene Betriebsrealität.

3.3. Landes- oder Verbundbetrieb als „Shared Service“ (anstelle FITKO)

Ein Landes- oder gemeinsames Rechenzentrum übernimmt den zentralen technischen Betrieb als Dienstleister für mehrere Länder (EfA-Prinzip). Die fachlich entscheidenden Behörden bleiben Verantwortliche. Der betreibende IT-Dienstleister wird Auftragsverarbeiter der Behörden. Die FITKO kann optional die Transportschicht bereitstellen und wäre dann zusätzlicher Auftragsverarbeiter. Grundlage sind länderübergreifende Verwaltungsvereinbarungen sowie abgestimmte Leistungs- und Sicherheitsstandards. Das Modell nutzt Skaleneffekte, erhält föderale Steuerung und erleichtert eine einheitliche Betriebs- und Sicherheitslinie. Es verlangt präzise vertragliche Steuerung, ein belastbares Unterauftragsmanagement und harmonisierte Release-Prozesse.

Wesentliche Anforderungen: AV-Verträge je Behörde mit dem Betreiber, optional ein zusätzlicher AV-Vertrag für die FITKO-Transportschicht. Eindeutige Regelung der Weisungen, Zuständigkeiten für TOM, Datenlokation, Exit- und Reversibilitätsmechanismen, Auditrechte und Eskalationslogik. Verbindliche Service-Level, abgestimmte Incident-Prozesse, ein zentrales Change- und Release-Management sowie ein transparentes Unterauftragsregister mit Genehmigungsprozessen.

Einschätzung: Aus Datenschutzsicht zulässig. Jedoch entsteht ein höherer Aufwand für zwischenstaatliche Abstimmung, Vereinbarungen und Governance und die Vorteile der föderalen Zusammenarbeit in der etablierten Struktur des IT-PLR werden nicht erreicht.

3.4. Gemeinsame Verantwortlichkeit nach Art. 26 DSGVO

Eine gemeinsame Verantwortlichkeit zwischen FITKO und nutzenden Behörden kommt nur in Betracht, wenn beide Seiten Zwecke und Mittel derselben Verarbeitung gemeinsam festlegen oder wenn das Fachrecht die FITKO ausdrücklich als mitverantwortliche Stelle bestimmt. Ohne eine tragfähige Rechtsgrundlage – die derzeit nicht besteht – für fachliche Verarbeitungen bei der FITKO ist dieses Modell für die Verarbeitung von Inhaltsdaten unzulässig.

Zulässig bleibt eine punktuelle gemeinsame Verantwortlichkeit für eng umschriebene, nichtfachliche Verarbeitungen, etwa für zentrale Sicherheits- oder Protokollierungsdienste, wenn beide Seiten die relevanten Zwecke und Mittel tatsächlich gemeinsam festlegen und eine Art. 26-Vereinbarung abschließen. In der Praxis erhöht dieses Modell den Abstimmungs- und Haftungsaufwand und sollte nur ausnahmsweise gewählt werden.

3.5. Zusammenfassung

Vorrangig und zu empfehlen bleibt das Modell eines zentralen Betriebs durch die FITKO mit ausgelagertem Hosting/technischen Betrieb (vorzugsweise mit Auftragsverarbeitung in Auftragskette). Andere Modelle sind datenschutzrechtlich darstellbar, führen allerdings zu höherem Abstimmungsaufwand und erreichen die Ziele der föderalen IT-Kooperation auf Basis von Art. 91c GG, wie sie auch im Beschluss des IT-PLR zur Neukonzeption von OSiP um Ausdruck kommen, nicht in gleicher Weise. Nicht zulässig wäre derzeitig mangels Rechtsgrundlage ein eigenverantwortlicher Betrieb durch die FITKO bzw. eine gemeinsame Verantwortlichkeit.

4. Technisch-organisatorische Maßnahmen

Frage: *„Welche rechtlichen Mindestanforderungen an technische und organisatorische Maßnahmen ergeben sich aus DSGVO, IT-Sicherheitsgesetz, BSI-Richtlinien oder KRITIS-Vorgaben für einen rechtssicheren Betrieb?"*

Kurzantwort:

Die Mindestanforderungen für den Betrieb von OSiP sind zwingend hoch (Art. 32 DSGVO), da die Verarbeitung Daten nach Art. 10 DSGVO (strafrechtliche Bezüge) betrifft.

Das Compliance-Rahmenwerk setzt sich aus folgenden drei zentralen Säulen zusammen:

1. Datenschutz-Compliance (DSGVO/DSK): Es ist die Einhaltung von Privacy by Design (Art. 25 DSGVO) und die Sicherstellung eines angemessenen Schutzniveaus (Art. 32 DSGVO) auf Basis einer DSFA (Art. 35 DSGVO) erforderlich. Die TOM sind entlang der Gewährleistungsziele des Standard-Datenschutz-Modells (SDM) zu strukturieren und umzusetzen, wobei nach den Vorgaben der Föderalen IT-Architekturrichtlinie die Referenzmaßnahmen des SDM nach Möglichkeit zu implementieren sind.
2. IT-Sicherheit (BSI/IT-PLR): Es muss der IT-Grundschutz des BSI angewendet werden. Verbindliche Vorgaben zur Kryptografie (E2EE-Verschlüsselung wird als Zielbild der DSK gefordert), Mandantentrennung und Protokollierung ergeben sich aus der Leitlinie Informationssicherheit und der Föderalen IT-Architekturrichtlinie des IT-Planungsrats.
3. KRITIS: Der IT-Dienstleister wird unter die Anforderungen der NIS2-Umsetzung fallen und muss ein entsprechendes Risikomanagement etablieren. Hierfür gelten die in der NIS2-VO (Umsetzungsverordnung) näher ausgeführten Kriterien.
4. Nachweis: Die Eignung der Auftragsverarbeiter muss vor Beauftragung durch Zertifikate (z.B. ISO/IEC 27001, ggf. auf Basis von IT-Grundschutz) nachgewiesen werden.

Alle Betrachtungsweisen (Datenschutz, IT-Sicherheit, KRITIS) setzen die Auswahl risikoangemessener TOM auf Basis einer Risikoanalyse voraus. Dabei ist davon auszugehen, dass für OSiP ein mindestens hoher Schutzbedarf zugrunde zu legen ist.

4.1. Datenschutz

4.1.1. Anforderungen der DSGVO (allgemein)

Als datenschutzrechtlich Verantwortliche müssen die OSiP nutzenden Stellen – d.h. insbesondere die zuständigen Behörden und die Erkenntnisstellen – sicherstellen, dass die Grundsätze der Verarbeitung gem. Art. 5 Abs. 1 DSGVO eingehalten werden. Sie müssen dies ferner jederzeit nachweisen können (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Hinsichtlich der technischen Gestaltung müssen die Verantwortlichen insbesondere die Einhaltung der folgenden Anforderungen nachweisen können:

- Privacy by Design (Art. 25 DSGVO): In der Designphase müssen risikoangemessene technisch-organisatorische Maßnahmen getroffen worden sein, um die Datenschutzgrundsätze wirksam umzusetzen.
- Sicherheit der Verarbeitung (Art. 32 DSGVO): Auf Basis einer Risikoanalyse müssen Verantwortliche und Auftragsverarbeiter angemessene technisch-organisatorische Maßnahmen (TOM) treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Maßnahmenauswahl sind der Stand der Technik, die Implementierungskosten, die Umstände und Eintrittswahrscheinlichkeit und Schwere der Risiken zu berücksichtigen.
- Sorgfältige Auswahl von Auftragsverarbeitern (Art. 28 Abs. 1 DSGVO): Verantwortliche müssen sich vor der Beauftragung von Auftragsverarbeitern vergewissern, dass diese hinreichende Gewähr dafür bieten, geeignete technische und organisatorische Maßnahmen zum Datenschutz durchzuführen.
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO): Die Verantwortlichen müssen ferner vor der Verarbeitung eine Datenschutz-Folgenabschätzung (DSFA) durchführen, wenn die Verarbeitung mit einem hohen Risiko verbunden ist. Hiervon ist bei OSiP auszugehen (s.o. 2). Im Rahmen der DSFA sollten einschlägigen Risikoszenarien identifiziert und die konkreten TOM abgeleitet werden.

4.1.2. Quellen zur Konkretisierung der Anforderungen

Die rechtlichen Mindestanforderungen an die TOM ergeben sich somit insbesondere aus Art. 25 und 32 DSGVO. Sie sind im Wesentlichen auf gesetzlicher Ebene nicht weiter konkretisiert. Es

gibt jedoch Quellen wie die Handreichungen der Datenschutz-Aufsichtsbehörden und im Bereich der Datensicherheit die Standards des BSI, die zur Auslegung der gesetzlichen Anforderungen herangezogen werden sollten. Insbesondere sollten folgende Dokumente beachtet werden:

4.1.2.1. Standard-Datenschutz-Modell (SDM)

Das von einer Untergruppe der Datenschutzkonferenz (DSK) entwickelte Standard-Datenschutz-Modell (SDM)[129] ist eine Vorgehensweise, mit der die rechtlichen Anforderungen aus der DSGVO in konkrete TOM übersetzt werden können. Nach der föderalen IT-Architekturrichtlinie sollen die Referenzmaßnahmen des SDM nach Möglichkeit umgesetzt werden (siehe I.1.2.2.5).

4.1.2.2. DSK, Entschließung zur E2EE

Die DSK fordert, im Bereich des E-Government auch bei Nutzung des Verbindungsnetzes (welches eine Transportverschlüsselung gewährleistet) ergänzend konsequent auf eine Ende-zu-Ende-Verschlüsselung zu setzen.[130] Sie fordert den IT-Planungsrat auf, entsprechende Standards wie OSCI-Transport kontinuierlich weiterzuentwickeln und verbindlich festzulegen.

4.1.2.3. Vorgehensmodell zur DSFA

Es gibt keine gesetzlich festgelegte Methodik für die Durchführung der DSFA. Der BayLfD hat eine Vorgehensweise für DSFA in der öffentlichen Verwaltung entwickelt, die auf dem SDM aufsetzt und sich daher vorliegend anbietet. Hierzu hat die Behörde Vorlagen und Handreichungen veröffentlicht.[131]

4.1.3. Konkretisierung der TOM

Es sind geeignete TOM umzusetzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl und Dimensionierung der TOM sind der Stand der Technik, die

---

129 https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

130 DSK, Entschließung vom 01. Oktober 2013 (86. Konferenz), „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln".

131 Siehe BayLfD, Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele, V1.0, 1. Mai 2022 und die weiteren Dokumente unter https://www.datenschutz-bayern.de/dsfa/.

Implementierungskosten sowie die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen (Art. 32 Abs. 1 DSGVO).

Das Projekt weist ein voraussichtlich hohes Risiko auf. Dies ergibt sich unter anderem daraus, dass für die Sicherheitsüberprüfung Daten über strafrechtliche Verurteilungen und Straftaten erfordert, die gem. Art. 10 DSGVO besonders geschützt sind. Daher sind die Mindestanforderungen an die TOM entsprechend höher anzusetzen.

Zur systematischen Umsetzung der DSGVO-Anforderungen sollten die TOM typischerweise anhand der Gewährleistungsziele des Standard-Datenschutzmodelles (SDM) strukturiert werden:

- **Verfügbarkeit, Integrität, Vertraulichkeit (Klassische Datensicherheitsziele)**
- **Datenminimierung, Nichtverkettung, Transparenz, Intervenierbarkeit** (Ziele zur Wahrung der Betroffenenrechte/Grundsätze nach Art. 5 DSGVO)

Zu jedem diese Ziele sind die typischen Risikoquellen zu berücksichtigen wie Mensch (z.B. Betriebspersonal, Hacker), Umwelt (Elementarschäden) und Anschlüsse (Strom, WAN) und die erwartbaren Risikoszenarien zu identifizieren. Jedes der Risikoszenarien ist mit TOM zu behandeln, bis das verbleibende Risiko akzeptabel ist. Nach den Vorgaben der IT-Architekturrichtlinie sind bei der Maßnahmenauswahl jedenfalls die Referenzmaßnahmen aus den SDM-Katalogen zu prüfen und nach Möglichkeit umzusetzen. Daher sind entlang der Gewährleistungsziele geeignete Referenzmaßnahmen aus den bislang veröffentlichen SDM-Bausteinen zu prüfen:

- Baustein 11: Aufbewahren[132]
- Baustein 41: Planen und Spezifizieren[133]
- Baustein 42: Dokumentieren[134]
- Baustein 43: Protokollieren[135]

---

132 DSK, SDM-Baustein 11 „Aufbewahren", V1.0 vom 06.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Aufbewahren_V1.0.pdf.

133 DSK, SDM-Baustein 41 „Planen und Spezifieren", V1.0 vom 25.03.2021, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Planen_Spezifizieren_V1.0.pdf.

134 DSK, SDM-Baustein 42 „Dokumentieren", V1.0a vom 02.09.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Dokumentieren_V1.0a.pdf.

135 DSK, SDM-Baustein 43 „Protokollieren", V1.0a vom 02.09.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf.

- Baustein 50: Trennen[136]
- Baustein 51: Zugriffe auf Daten, Systeme und Prozesse regeln[137]
- Baustein 60: Löschen und Vernichten[138]
- Baustein 61: Berichtigen[139]
- Baustein 62: Einschränken der Verarbeitung[140]

Die sich aus Datenschutzsicht ergebenden TOM können hier nicht abschließend wiedergegeben werden. Eine tabellarische Übersicht über wesentliche Anforderungen auf Basis des SDM und von IT-Grundschutz – ohne Anspruch auf Vollständigkeit – fügen wir an als Anlage 5.

4.2. IT-Sicherheit

4.2.1. Anzuwendende Regelungen

Im Bereich der IT-Sicherheit sind insbesondere die folgenden Regelwerke bei der Gestaltung von OSiP zu beachten.

4.2.1.1. Leitlinie Informationssicherheit (IT-PLR)

Die Leitlinie ist vom IT-Planungsrat beschlossen und gilt bei ebenenübergreifenden Projekten wie OSiP für alle beteiligten Stellen der öffentlichen Verwaltung. Durch die Umsetzungsgesetze der Länder hat diese Vorgabe für die Behörden der Länder Gesetzeskraft (siehe I.1.2.2.3). Bei

---

136 DSK, SDM-Baustein 50 „Trennen", V1.0 vom 06.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf.

137 DSK, SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" (V1.0 vom 01.11.2021), https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Zugriffe_regeln_V1.0.pdf.

138 DSK, SDM-Baustein 60 „Löschen und Vernichten" (V1.0a vom 02.09.2020), https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf.

139 DSK, SDM-Baustein 61 „Berichtigen" (V1.0 vom 06.10.2020), https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Berichtigen_V1.0.pdf.

140 DSK, SDM-Baustein 62 „Einschränken der Verarbeitung" (V1.0 vom 06.10.2020), https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Einschr%C3%A4nken_V1.0.pdf.

ebenenübergreifenden Verfahren, die von Bund, Ländern und Kommunen gemeinsam betrieben oder genutzt werden, gelten die Regelungen der Leitlinie beim Anschluss an den Informationsverbund, also für sämtliche nutzenden und bereitstellenden Stellen.[141]

Die Leitlinie formuliert Mindestanforderungen, die sich am IT-Grundschutz des BSI, dem IT-Grundschutz-Kompendium und der ISO 2700x-Normreihe orientieren.[142] Die Anforderungen betreffen folgende Handlungsfelder:

- Informationssicherheitsmanagement
- Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung
- Einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren
- Gemeinsame Abwehr von IT-Angriffen
- IT-Notfallmanagement

Bei der Auftragsvergabe an Dritte, die Leistungen für die öffentliche Verwaltung erbringen, sind diese auf die verbindlichen Vorgaben der Leitlinie zu verpflichten.[143]

Zum Erreichen der Ziele der Leitlinie hat die AG Informationssicherheit des IT-PLR einen Umsetzungsplan erlassen, den der IT-PLR beschlossen hat.[144] Der Umsetzungsplan behandelt die Handlungsfelder 1-5 der Informationssicherheits-Leitlinie. Zum Handlungsfeld 3 „Einheitliches Sicherheitsniveau für ebenen übergreifende IT-Verfahren" sieht er unter anderem vor

- dass bei Planung, Aufbau und Anpassung ebenenübergreifender IT-Verfahren der IT-Grundschutz des BSI in der jeweils gültigen Fassung anzuwenden ist,[145]
- dass der Verantwortliche für das Verfahren die IT-Architektur und die Anforderungen nach IT-Grundschutz unter Berücksichtigung der zu erwartenden Zielgruppe in der Verwaltung für die Nutzung der Anwendung festlegt,

---

141 Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 2.

142 Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 5.

143 Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 5.

144 IT-PLR, Beschluss 2020/05 vom 25.03.2020.

145 AG InfoSic des IT-PLR, Umsetzungsplan zur Leitlinie Informationssicherheit, V1.0 vom 05.02.2020, Ziffer 3.2.

- dass für die tatsächliche Umsetzung des IT-Grundschutzes durch den Verantwortlichen für das IT-Verfahren ein geeigneter Nachweis geführt wird.

4.2.1.2. Föderale IT-Architekturrichtlinie

Die Leitlinie ist vom IT-Planungsrat beschlossen. Die darin enthaltenen Vorgaben zur Informationssicherheit sind für föderale Projekte wie OSiP verbindlich. Dies gilt auch für die aus der nationalen IT-Architekturrichtlinie übernommen Vorgaben, sodass auf diesem Weg im Ergebnis auch die referenzierten BSI-Mindeststandards, die unmittelbar nur für Bundesbehörden gelten, verbindlich sind. Mit Blick auf die IT-Sicherheit sind insbesondere folgende Anforderungen hervorzuheben:

- AV-08 „Sicherheit und Schutz“[146] mit Verweis auf folgende weitere Regelungen zur IT-Sicherheit:
    - BSI 200-1 ISMS
    - BSI 200-2 Grundschutz
    - BSI 200-3 Risikoanalyse
    - BSIG
    - BSI Info
    - Nato Cyber Defence
- FV-08 „Schutz“[147], wonach u.a. verlangt wird:
    - ein Informationssicherheitskonzept nach BSI-Grundschutz zu erstellen, umzusetzen und regelmäßig zu auditieren;
    - passfähige Trennungs- und Vertrauensmechanismen (inklusive Separierung, Segmentierung und Mandantentrennung).
- TV-08 „Protektion“[148] verlangt technische Sicherheitssysteme folgender Art:

---

146 IT-PLR, Föderale IT-Architekturrichtlinie, V1.9.0, AV-08 Sicherheit und Schutz, S. 23.

147 IT-PLR, Föderale IT-Architekturrichtlinie, V1.9.0, FV-08 Schutz, S. 42.

148 IT-PLR, Föderale IT-Architekturrichtlinie, V1.9.0, FV-08 Schutz, S. 52.

- Kryptografische Verfahren nach dem Stand der Technik (BSI TR-02102, BSI TR-03116)
- Protokollierung von Ereignissen und Detektion von Cyberangriffen (u.a. BSI Mindeststandard Protokollierung und Detektion, BSI OPS.1.1.5 Protokollierung, BSI DER.1 Detektion)
- Virenschutz und Schadprogrammabwehr nach aktuellem Stand der Technik (u.a. OPS.1.1.4 Schadprogramme)

4.2.1.3. IT-Grundschutz des BSI

Gemäß der Leitlinie Informationssicherheit (IT-PLR) ist bei Planung und Anpassung ebenenübergreifender IT-Verfahren – wie OSiP – der IT-Grundschutz des BSI in seiner jeweiligen Fassung anzuwenden.[149]

4.2.1.4. Informationssicherheitsleitlinie der FITKO

Neben den vom IT-Planungsrat beschlossenen Leitlinien und Richtlinien gilt für OSiP als FITKO-Produkt die „Informationssicherheitsleitlinie der FITKO" (Version 1.0, 2023). Sie legt für alle FITKO-Produkte verbindliche Mindestanforderungen an Organisation, Prozesse und technische Maßnahmen der Informationssicherheit fest und orientiert sich inhaltlich an der Leitlinie Informationssicherheit des IT-Planungsrats, dem IT-Grundschutz des BSI und den ISO-Zertifizierungen.

Für OSiP bedeutet dies, dass die in der FITKO-Informationssicherheitsleitlinie definierten Vorgaben, insbesondere zu Rollen und Verantwortlichkeiten (z. B. Informationssicherheitsbeauftragter, Produktverantwortung), zum Aufbau und Betrieb eines ISMS, zum Risikomanagement sowie zu technischen und organisatorischen Sicherheitsmaßnahmen, im Architektur-, Betriebs- und Sicherheitskonzept verbindlich zu berücksichtigen sind. Bei der Beauftragung externer IT-Dienstleister ist sicherzustellen, dass deren Sicherheitsorganisation und TOM die Anforderungen der FITKO-Informationssicherheitsleitlinie abdecken und vertraglich entsprechend verpflichtend gemacht werden.

---

149 Leitlinie Informationssicherheit (IT-PLR), Version 2.0, 06.12.2018, Ziffer 5.3.

4.2.2. Weitere Regelungen

Folgende Regelwerke sind (voraussichtlich) formal nicht unmittelbar bindend, können aber ggf. zur Ableitung von TOM herangezogen werden.

4.2.2.1. Informationssicherheitsrichtlinie ITKB (ISR ITKB)

Die Leitlinie ist verbindlich für die Bundesbehörden. Ihr Geltungsbereich umfasst OSiP formal dann, wenn OSiP in die IT-Dienstekonsolidierung (DK) einbezogen und den Bundesbehörden zentral über die DK bereitgestellt wird (siehe I.1.2.3.4.3). Wir gehen grundsätzlich davon aus, dass OSiP als Produkt der FITKO im Rahmen der föderalen IT-Zusammenarbeit nicht Teil der IT-Konsolidierung des Bundes sein soll und die ISR ITKB daher nicht – jedenfalls nicht unmittelbar – gilt.

4.2.2.2. BSI, Positionspaper Zero Trust 2023[150]

Der Beschluss des IT-PLR zur Neukonzeption von OSiP nennt als Architekturziel einen Zero-Trust-Ansatz.[151] Es ist zu empfehlen, das (unverbindliche) Positionspapier des BSI heranzuziehen, um das Architekturdesign-Paradigma „Zero Trust" in konkrete Anforderungen an die Architektur zu überführen und konkrete TOM abzuleiten.

4.2.2.3. Mindeststandards des BSI

Die Mindeststandards des BSI gelten im Zweifel weder nach der aktuellen Rechtslage (siehe 4.2.2.3.1) noch nach der zukünftigen Rechtslage (siehe 4.2.2.3.2) unmittelbar für die FITKO bzw. den von ihr beauftragten IT-Dienstleister von OSiP. Jedoch ist eine Orientierung an den Mindeststandards gleichwohl sinnvoll, um bei ebenenübergreifenden Verfahren ein einheitliches IT-Sicherheitsniveau zu gewährleisten. Dies entspricht auch dem Bestreben der AG InfoSic des IT-PLR bei der Umsetzung der Leitlinie Informationssicherheit.[152]

---

150 BSI, Positionspapier Zero Trust 2023, V1.12 vom 26.06.2023.

151 IT-PLR, Beschluss 2025/20 vom 26.03.2025, Ziffer 2.1.

152 Vgl. AG InfoSic des IT-PLR, Umsetzungsplan zur Leitlinie Informationssicherheit, V1.0 vom 05.02.2020, Ziffer 3.3.

4.2.2.3.1. § 8 BSIG (noch geltende Rechtslage)

Die Geltung der Mindeststandards des BSI wurde 2021 auch auf öffentliche Unternehmen ausgeweitet, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen (§ 8 Abs. 1 Satz 1 Nr. 3 BSIG).[153]

Für die FITKO gilt diese Regelung nicht, da die FITKO als AöR organisiert ist und der Bund nicht mehrheitlich beteiligt ist. Für den zentralen Dienstleister würde die Regelung nur gelten, wenn dieser ein öffentliches Unternehmen im Mehrheitseigentum des Bundes ist (z.B. BWI GmbH)[154]; für einen Landes-IT-Dienstleister wie Dataport würde sie hingegen nicht (unmittelbar) gelten. Nach der derzeitigen gesetzlichen Regelung ergibt sich also voraussichtlich keine unmittelbare Anwendung der Mindeststandards nach § 8 BSIG auf die FITKO und den zentralen technischen Betreiber von OSiP. Jedoch ist mit der baldigen Novellierung des BSIG im Zuge der NIS2-Umsetzung zu rechnen (dazu sogleich).

4.2.2.3.2. § 29 BSIG-E (zukünftige Rechtslage)

Nach der geplanten NIS2-Umsetzung gelten zukünftig „öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung" als Einrichtungen der Bundesverwaltung (§ 29 Abs. 1 Nr. 2 BSIG-E). Auf sie sind damit gem. § 29 Abs. 2 BSIG-E Teile der Vorschriften für „besonders wichtige Einrichtungen" (KRITIS) anzuwenden. Hierzu gehört die Pflicht, die Mindeststandards des BSI einzuhalten (§ 44 BSIG-E).

Die FITKO und ein von ihr beauftragter IT-Dienstleister für OSiP sind im Zweifel auch von der Neuregelung des § 29 BSIG-E nicht erfasst. Zwar sind sie „öffentlich-rechtlich organisierte IT-Dienstleister". Jedoch sind sie im Zweifel keine „IT-Dienstleister der Bundesverwaltung" im Sinne von § 29 BSIG-E. Die Formulierung legt eine organisatorische Eingliederung in die Bundesverwaltung nahe und nicht lediglich das Erbringen von IT-Dienstleistungen für die Bundesverwaltung. Dies ergibt sich gerade auch in der Gegenüberstellung zu der Formulierung aus § 8 Abs. 1 Satz 1 Nr. 3 BSIG in der aktuellen Fassung. Im Zweifel ist daher davon auszugehen, dass die Mindeststandards des BSI im Rahmen des Angebots von OSiP nicht über § 29 BSIG-E unmittelbar für die FITKO bzw. den zentralen IT-Dienstleister gelten (siehe aber zur Anwendung der KRITIS-Regelungen auf den IT-Dienstleister 4.3.3.1).

---

153 BT-Drs. 19/26106, S. 78.

154 Vgl. Brandenburg in Kipker/Reusch/Ritter, § 8 BSIG Rn. 10.

4.2.3. Konkretisierung

OSiP verarbeitet Daten mit hohem Schutzbedarf. Es ist zudem davon auszugehen, dass Erkenntnisstellen jedenfalls zum Teil auch Erkenntnisse über OSiP übermitteln sollen, die als VS-NfD eingestuft sind. Ausgehend von diesem Schutzbedarf werden in Anlage 5 einige wesentliche Anforderungen hinsichtlich der IT-Sicherheit (und des Datenschutzes) wiedergegeben. Für ein vollständige Liste muss auf die o.g. und referenzierten Dokumente verweisen werden.

4.3. KRITIS

4.3.1. OSiP als „kritischer Verwaltungsprozess" im Sinne der Leitlinie Informationssicherheit (IT-PLR)

Es ist davon auszugehen, dass OSiP im Sinne der Leitlinie Informationssicherheit (IT-PLR) ein „kritischer IT-gestützter Verwaltungsprozess" ist, für den erhöhte Sicherheitsanforderungen gelten.

Nach der Definition der Leitlinie sind kritische IT-Prozesse solche, die „für die Arbeitsfähigkeit der Verwaltung von essentieller Bedeutung sind". Die Durchführung von Zuverlässigkeits- und Sicherheitsüberprüfungen ist eine zentrale und essentielle staatliche Aufgabe, die zur Sicherstellung der inneren und äußeren Sicherheit beiträgt. Beeinträchtigungen der Sicherheit könnten erhebliche Auswirkungen haben:

- Verfügbarkeit: Der Ausfall oder die Beeinträchtigung der Verfügbarkeit dieses Prozesses würde zu erheblichen Einschränkungen der Handlungsfähigkeit der beteiligten öffentlichen Stellen führen.
- Vertraulichkeit: Die Kompromittierung der Vertraulichkeit der ausgetauschten Informationen würde potentiell erhebliche Beeinträchtigungen für die Betroffenen und ggf. die durch die Prüfung zu schützenden staatlichen Institutionen bedeuten.
- Integrität: Schließlich würde eine Beeinträchtigung der Integrität ggf. zu fehlerhaften Prüfung führen und damit die Schutzzwecke der diversen Rechtsgrundlagen (z.B. WaffenG, LuftsicherheitsG) erheblich gefährden und somit ggf. zu einer Beeinträchtigung von Leib und Leben führen.

Diese möglichen Schadensfolgen implizieren einen hohen Schutzbedarf oder sogar sehr hohen Schutzbedarf.[155] Somit ist von einem kritischen IT-gestützten Verwaltungsprozess im Sinne der Leitlinie auszugehen. Mithin ergeben sich nach der Leitlinie über das ohnehin geforderte Sicherheitsniveau hinaus besondere Sicherheitsanforderungen für OSiP, insbesondere hinsichtlich

- Netzwerkverbindungen: Die Leitlinie strebt für kritische ebenenübergreifende Verwaltungsprozesse einen „durchgängig hohen Schutzbedarf für Netzwerkverbindungen" an (Ziffer 5.2 der Leitlinie).
- Notfallvorsorge: Bei kritischen ebenenübergreifenden IT-Verfahren ist im Rahmen der Notfallvorsorge ein Prozess zu etablieren, welcher festlegt, ob und welche gemeinsamen Rückfallebenen für das jeweilige IT-Verfahren notwendig und möglich sind.

4.3.2. KRITIS – bisherige Regelung (NIS-RL/BSIG/BSI-KritisV)

Nach der derzeit noch geltenden Rechtslage richten sich die KRITIS-Regelungen an bestimmte Sektoren der Wirtschaft, die kritische Dienstleistungen der Allgemeinheit erbringen (Energie, Wasser, Ernährung, Gesundheit, Transport und Verkehr, Entsorgung, IT und TK, Finanzen und Versicherungen). Die diesen Sektoren zugehörigen „Kritischen Infrastrukturen" (KRITIS, vgl. § 2 Abs. 10 BSIG), die bestimmte Größen überschreiten und daher von hoher Bedeutung für das Funktionieren des Gemeinswesen sind, sind besonderen Sicherheitsanforderungen unterworfen (§ 8a BSIG). Ähnliche Anforderungen gelten für „Unternehmen im besonderen öffentlichen Interesse" (§ 2 Abs. 14 BSIG), d.h. sehr große Unternehmen und Betreiber von Betriebsbereichen der oberen Klasse gemäß Störfall Verordnung (z.B. AKW-Betreiber).

Da die öffentliche Verwaltung als solche von den bisherigen KRITIS-Regelungen nicht erfasst war, ergeben sich aus den bisherigen Regelungen keine besonderen Anforderungen für OSiP. Allerdings gilt mittlerweile die NIS2-Richtlinie, die voraussichtlich Ende 2025/Anfang 2026 in deutsches Recht umgesetzt wird und daher für OSiP relevanter ist (dazu sogleich).

---

155 Vgl. BSI-Standard 200-2, V1.0, S. 106 f.

4.3.3. KRITIS – zukünftige Regelung (NIS2-RL/BSIG-E/KritisDachG-E)

4.3.3.1. Anwendbarkeit der KRITIS-Regelungen auf den Betreiber

Durch die Neufassung des BSI-G im Zuge der Umsetzung der NIS2-Richtlinie wird der Anwendungsbereich der KRITIS-Regelungen an die NIS-Richtlinie angepasst und erweitert.

Angesichts der typischen Tätigkeit und Größe eines IT-Dienstleisters, der für den Betrieb von OSiP in Frage kommt, ist im Zweifel davon auszugehen, dass dieser als besonders wichtige Einrichtung oder jedenfalls wichtige Einrichtung einzustufen im Sinne der neuen KRITIS-Regelung einzustufen sein wird. Insbesondere fallen unter die geregelten Sektoren zukünftig Anbieter „Digitaler Infrastruktur" gem. § 28 Abs. 1 BSIG-E iVm Anlage 1 Ziffer 6 BSIG-E. Es ist davon auszugehen, dass der mit dem Betrieb von OSiP beauftragte Dienstleister in mindestens eine der folgenden Unterkategorien fällt:

- Managed Services Provider (§ 2 Nr. 26 BSIG-E und Anlage 1 Ziffer 6.1.10)
- Managed Security Services Provider (§ 2 Nr. 25 BSIG-E und Anlage 1 Ziffer 6.1.11)
- Rechenzentrumsdienst (§ 2 Nr. 35 BSIG-E und Anlage 1 Ziffer 6.1.5)
- Cloud-Computing-Dienst (§ 2 Nr. 4 BSIG-E und Anlage 1 Ziffer 6.1.4)

Sofern der Dienstleister in eine der genannten Kategorien fällt und zugleich die nachstehend genannten Schwellwerte überschreitet, fällt er unter die KRITIS-Regelungen. Insbesondere ist der Dienstleister eine

- besonders wichtige Einrichtung (§ 28 Abs. 1 Satz 1 Nr. 4 BSIG-E), sofern er
    - mindestens 250 Mitarbeiter beschäftigt oder
    - einen Jahresumsatz von über 50 Millionen Euro und eine Jahresbilanzsumme von über 43 Millionen Euro aufweist;
- wichtige Einrichtung (§ 28 Abs. 2 Satz 1 Nr. 3 BSIG-E), sofern er
    - mindestens 50 Mitarbeiter beschäftigt oder
    - einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweist.

Die Einstufung als besonders wichtige Einrichtung oder wichtige Einrichtung gilt allerdings nicht, sofern der Dienstleister zugleich eine Einrichtung der Bundesverwaltung ist (insbesondere ein öffentlich-rechtlich organisierter IT-Dienstleister der Bundesverwaltung nach § 29 Abs. 1

Nr. 3 BSIG-E). In diesem Fall gelten für ihn nicht sämtliche Anforderungen von KRITIS, sondern „nur" die Anforderungen an Einrichtungen der Bundesverwaltung nach § 29 BSIG-E (dazu 4.2.2.3.2), also u.a. die Mindeststandards des BSI.

4.3.3.2. Inhalt der KRITIS-Regelungen

Sofern der Dienstleister nach den o.g. Vorschriften als besonders wichtige Einrichtung oder wichtige Einrichtung einzustufen ist gelten nach §§ 30 ff. BSIG-E besondere Anforderungen an das Risikomanagement sowie die Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten des IT-Anbieters. Diese Pflichten sind nicht OSiP-spezifisch, d.h. sie gelten für den IT-Dienstleister schon aufgrund seiner Tätigkeit und Größe. Die in Betracht kommenden IT-Dienstleister müssen also mit Blick auf NIS2 ihre Organisation ohnehin an die Vorgaben der §§ 30 ff. BISG-E anpassen. Jedoch muss das zu betreibende Risikomanagement im Falle eines OSiP-Betriebs auch die damit zusammenhängenden Leistungen erfassen.

Für das Risikomanagement ergeben sich aus § 30 BSIG-E folgende Anforderungen:

- Abs. 1: Es sind geeignete, verhältnismäßige und wirksame TOM zu ergreifen zum Schutz der für die Dienstleistung genutzten IT-Systeme, Komponenten und Prozesse. Bei der Maßnahmenauswahl sind Risikoexposition, Größe der Einrichtung, Umsetzungskosten, Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.
- Abs. 2: Die TOM müssen den Stand der Technik einhalten, einschlägige europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen. Sie müssen mindestens folgende Bereiche umfassen:
    - Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
    - Bewältigung von Sicherheitsvorfällen,
    - Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
    - Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,

- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
- Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Für Anbieter von Rechenzentrumsdiensten (und weiteren Diensten mit vergleichbaren Anforderungen an die IT-Sicherheit) hat die EU-Kommission eine Durchführungsverordnung erlassen, welche die technischen und methodischen Anforderungen an das Risikomanagement weiter konkretisier (dazu sogleich 4.3.4.)

4.3.4. Durchführungsverordnung (EU) 2024/2690

Nach der Durchführungsverordnung (EU) 2024/2690 (NIS2-UmsVO oder kurz NI2-VO) müssen die von dieser Verordnung betroffenen Einrichtungen – wozu u.a. Betreiber von Rechenzentren gehören – das ihnen nach KRITIS vorgeschriebene Risikomanagement (4.3.3.) unter Berücksichtigung der technischen und methodischen Anforderungen im Anhang der NSI2-VO umsetzen. Der Anhang der NIS2-VO ist daher vom OSiP-Betreiber im Rahmen seiner NIS2-Umsetzung besonders zu beachten. Konkret enthält der Angang Vorgaben für

- das Konzept für die Sicherheit von Netz- und Informationssystemen, einschließlich der Rollen, Verantwortlichkeiten und Weisungsbefugnisse,
- das Risikomanagement, nämlich für den Risikomanagementrahmen, die Überwachung der Einhaltung und die unabhängige Überprüfung der Netz- und Informationssicherheit,

- die Bewältigung von Sicherheitsvorfällen, genauer für das entsprechende Konzept, die Überwachung und Protokollierung, die Meldung von Ereignissen, deren Bewertung und Klassifizierung, die Reaktion auf Sicherheitsvorfälle und die Überprüfungen nach Sicherheitsvorfällen,
- das Betriebskontinuitäts- und Krisenmanagement, insbesondere den Notfallplan, das Backup-Sicherungs- und Redundanzmanagement und das Krisenmanagement,
- die Sicherheit der Lieferkette, durch ein Konzept und ein Anbieterverzeichnis,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Vorgaben für einen sicheren Entwicklungszyklus, das Konfigurationsmanagement, das Änderungsmanagement, Reparatur und Wartung, die Sicherheitsüberprüfung, das Sicherheitspatch-Management, die Netzsicherheit, die Netzsegmentierung, den Schutz gegen Schadsoftware und nicht genehmigte Software, die Behandlung und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen zur Cybersicherheit,
- Kryptografie, d.h. ein risikoangemessenes Kryptokonzept und -verfahren, dass die Algorithmen und Parameter der Kryptografie, ggf. einen Krypto-Agilitätsansatz und das Schlüsselmanagement umfasst und das in regelmäßigen Zeitabständen aktualisiert wird,
- die Sicherheit des Personals einschließlich von Zuverlässigkeitsüberprüfungen, Offboading-Management und Disziplinarverfahren,
- die Zugriffskontrolle, d.h. das Zugriffskonzept, das Management von Zugang- und Zugriffsrechten, die privilegierten Konten und die Systemverwaltungskonten, die Systemverwaltungssysteme, die Identifizierung, die Authentizifierung, die Multifaktor-Authentifizierung,
- das Anlagen- und Wertemanagement, d.h. die Anlagen- und Werteklassifizierung, die Behandlung von Anlagen und Werten, das Konzept für Wechseldatenträger, das Anlagen- und Werteinventar und die Abgabe, Rückgabe oder Löschung von Anlagen und Werten bei Beendigung des Beschäftigungsverhältnisses, und

- die Sicherheit des Umfelds und physische Sicherheit, d.h. die unterstützenden Versorgungsleistungen, den Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds, Perimeter und physische Zutrittskontrolle,

Zu allen genannten Punkten finden sich im Anhang der NIS2-VO nähere Anforderungen in Form von kurzen Anforderungskatalogen. Damit wird das Risikomanagementsystem also bereits relativ konkret beschrieben. Die Anforderungen laufen teils parallel mit Anforderungen, die sich etwa nach ISO 27001 oder konkret dem IT-Grundschutz ergeben, sodass in der Praxis auch die implementierten TOM sich weithin überschneiden. Gleichwohl müssen die KRITIS Anforderungen von betroffenen RZ-Dienstleistern (wie dem OSiP-Betreiber) für sich betrachtet, analysiert und vollständig umgesetzt werden, wobei insbesondere auch der abstrakt hohe Schutzbedarf durch die Einstufung als „wichtige Einrichtung“ oder „besonders wichtige Einrichtung“ zu berücksichtigen ist.

5. Einsatz von Adaptern (Format-Konvertierung)

Fragen: „*Wie ist der Betrieb von E2EE-unterbrechenden Format-Adaptern (siehe B.VI.3.) durch die FITKO (als Auftragsverarbeiter) datenschutzrechtlich zu bewerten? Ist dieser Betrieb mit den Zielen „Privacy by Design" und dem Zero-Trust-Ansatz vereinbar? Welches Betriebsmodell wird für die Entwicklung und Betrieb von Adaptern empfohlen? Können und sollten diese im Auftrag der* FITKO *betrieben werden, oder sollte die Betriebsverantwortung für diese bei anderen Stellen liegen? Inwiefern ändern sich die Einschätzungen, falls diese Adapter Daten nicht nur konvertieren, sondern auch persistieren? Welche Rolle spielt dabei die Auswahl der gehaltenen Daten?*"

Kurzantwort:

Der Einsatz von Adaptern (Format-Konvertierern) unterbricht die Verschlüsselung zwischen Sender und Empfänger und widerspricht damit einer strengen E2EE.

Bei E2EE handelt es sich allerdings nicht um eine zwingende datenschutzrechtliche Vorgabe. Vielmehr ist E2EE „lediglich" eine hochwirksame und damit grundsätzlich sehr relevante und hoch zu priorisierende TOM. Sie kann aber auch bei Nachrichten mit hohem Schutzbedarf ggf. durch andere Sicherheitsmaßnahme kompensiert werden. Maßgeblich ist die unter Berücksichtigung aller Umstände vorzunehmende Risikoanalyse und eine Maßnahmenauswahl unter Beachtung der Vorgaben von Art. 32 DSGVO. Bei entsprechender Begründung widerspricht ein Verzicht auf E2EE auch nicht den Grundsätzen von Privacy by Design und Zero Trust.

Zu empfehlen ist ersatzweise eine Gateway-zu-Gateway-Verschlüsselung (G2GE) oder Gateway-zu-Ende-Verschlüsselung (G2EE), um jedenfalls den Weg zwischen der sendenden und der empfangenden verantwortlichen Stelle abzusichern und den Dienstleister von jedem Zugriff auf den Nachrichteninhalt technisch auszuschließen. Daher sollte ein Adapter durch die sendende Stelle betrieben werden (bzw. je nach technischer Erforderlichkeit oder Gestaltung durch die empfangende Stelle) und ein Dienstleister – wenn unbedingt erforderlich zu Wartungszwecken – nur ausnahmsweise im Rahmen einer Auftragsverarbeitung auf den Adapter (Server) Zugriff nehmen.

Eine Persistierung von Daten auf dem Adapter ist nach den Grundsätzen von Datensparsamkeit und Speicherbegrenzung zu vermeiden.

5.1. E2EE-Verschlüsselung

Der Einsatz von Ende-zu-Ende-Verschlüsselung (E2EE) ist eine der vom IT-PLR formulierten Leitziele der Neukonzeption von OSiP (**Fehler! Verweisquelle konnte nicht gefunden werden.**). Vor diesem Hintergrund stellt sich die Frage, wie sich der Einsatz von Adapter (iSv Format-Konvertierern), zu der Forderung einer E2EE verhält.

5.1.1. Definition E2EE

Zur Definition der E2EE kann auf die in der Diskussion um das besondere elektronische Anwaltspostfach (beA) hierzu zitierte Patenschrift EP 0 877 507 B1 zurückgegriffen werden.[156] Darin heißt es:

> *„Unter der Bezeichnung Ende-zu-Ende Verschlüsselung (End-To-End-Encryption – ETEE) versteht man die Möglichkeit zum uni- oder bidirektionalen Austausch von Informationen (insbesondere Sprache aber auch Fax oder Daten) zwischen zwei Teilnehmern innerhalb eines digitalen Kommunikationssystems in verschlüsselter Form. Charakteristisch ist hierbei die Verschlüsselung am Ort des Senders und die Entschlüsselung erst beim Empfänger einer Nachricht wobei der dazwischenliegende Kommunikationskanal keinen Einfluß auf die Chiffrierung besitzt. Innerhalb der digitalen Übertragungskette existiert keine Möglichkeit zur Umwandlung der Nachricht in den ursprünglichen Klartext."* (sic)

Im Detail ergeben sich technische Fragen dahingehend, was genau unter dem Endpunkt der Kommunikation zu verstehen ist.[157] Für die Zwecke dieses Gutachtens ist die vorstehende Definition jedoch ausreichend (und wurde daher u.a. vom BGH in der Rechtsprechung zum beA verwendet).

Zu unterscheiden ist die E2EE jedenfalls von einer Gateway-to-Gateway-Encryption (teils auch G2GE genannt).[158] Dabei findet die Verschlüsselung nicht zwischen den Endpunkten, sondern

---

[156] Abrufbar unter: https://register.epo.org/application?number=EP98108118.

[157] Siehe den mittlerweile obsoleten Entwurf der IETF zu Definition von E2EE aus 2023: IETF, Internet-Draft „draft-knodel-e2ee-definition-11", Abrufbar unter https://www.ietf.org/archive/id/draft-knodel-e2ee-definition-11.html.

[158] Siehe schon IETF, https://www.rfc-editor.org/rfc/rfc1825.html, S. 4.

z.B. zwischen Gateways statt, die die internen Netzwerke der Kommunikationspartner vom Internet (oder einem WAN) trennen. Die G2GE – z.B. in Form eines VPN – schützt wie die E2EE wirksam gegen Zugriff von Dritten auf dem öffentlichen Teil der Übertragungsstrecke, jedoch nicht vor Zugriffen auf den Gateways (oder der Strecke zwischen dem Rechner des Endnutzers und dem Gateway). Dafür ermöglichen sie, sofern keine weitere Verschlüsselung eingesetzt wird, Schutzmaßnahmen in Form einer Inhaltsprüfung der Nachrichten am Gateway (z.B. Firewall mit Packet Inspection).

5.1.2. Notwendige Unterbrechung der E2EE durch Adapter

Adapter (Format-Konvertierer) unterbrechen notwendig die Verschlüsselungsstrecke, da die Daten für die Format-Konvertierung im Klartext vorliegen müssen. Operationen auf verschlüsselten Daten sind nur in eng begrenzten Anwendungsfällen durchführbar (sog. homomorphe Verschlüsselung), die vorliegend nicht gegeben sind. Eine Verschlüsselung kann vorliegend also nicht zwischen Sender (Client) zum Empfänger (Client) erreicht werden, sondern maximal vom Sender zum Adapter und vom Adapter zum Empfänger. Bei Einsatz von Adapter ist mithin eine E2EE nach dem klassischen, strengen Verständnis nicht möglich.

Möglich bleibt aber etwa eine G2GE oder G2EE (wenn der Adapter als Gateway im Netz des Senders/Empfängers steht).

5.1.3. E2EE als hochwirksame und empfohlene Maßnahme

Wie gesehen vereinfacht eine E2EE zudem die datenschutzrechtliche Bewertung, da verschlüsselte Daten für einen Dienstleister, der keine realistische Möglichkeit zur Entschlüsselung hat, keinen Personenbezug aufweisen (1.2.2.2.). Schließlich ist eine E2EE eine hochwirksame technisch-organisatorische Schutzmaßnahme, die regelmäßig von Datenschutz-Aufsichtsbehörden empfohlen oder gefordert wird,[159] auch konkret als zusätzliche Maßnahme bei Übermittlungen über das Verbindungsnetz (**Fehler! Verweisquelle konnte nicht gefunden werden.**.).[160]

---

[159] Vgl. DSK, Gewährleistung der Menschenrechte bei der elektronischen Kommunikation, Entschließung vom 27.03.2014 (87. Konferenz), Forderung Nr. 3.

[160] Vgl. DSK, Sichere elektronische Kommunikation gewährleisten, Beschluss vom 02.10.2013 (86. Konferenz).

5.1.4. E2EE ist aus Datenschutzsicht jedoch nicht alternativlos

Trotz des hohen sicherheitstechnischen Nutzens einer E2EE ist festzuhalten, dass die Forderung nach einer E2EE aus Datenschutzsicht keinen Absolutheitsanspruch hat. Vielmehr verlangt das Datenschutzrecht, risikoangemessene Maßnahmen zu treffen, um u.a. Vertraulichkeit zu gewährleisten (siehe Art. 32 Abs. 1 DSGVO; **Fehler! Verweisquelle konnte nicht gefunden werden.**; **Fehler! Verweisquelle konnte nicht gefunden werden.**). Da E2EE im Allgemeinen eine hochwirksame Maßnahme zur Erreichung dieses Schutzziels ist, ist sie gerade bei Daten mit hohem Schutzbedarf regelmäßig besonders geeignet und zu empfehlen. Sie gilt daher auch als besonders relevante Maßnahme zur Einhaltung der Anforderungen an Privacy by Design.[161]

Zwingend geboten ist eine E2EE aber nur dann, wenn die Risikoanalyse und Maßnahmenplanung zu dem Ergebnis kommt, dass unter den konkreten Umständen für die beabsichtigte Verarbeitung keine anderen, hinreichend wirksamen Schutzmaßnahmen zur Verfügung stehen. Liegt ein solcher Fall nicht vor, kann der Verzicht auf E2EE durch andere Schutzmaßnahmen, die die bestehenden Risiken hinreichend verringern, kompensiert werden.

Zudem kann es – je nach den Umständen – Erfordernisse geben, die mit einer E2EE nicht kompatibel sind und einen Verzicht rechtfertigen:

- Ein Beispiel ist die gewünschte Prüfung auf Schadsoftware bei De-Mail und die Möglichkeit zur Verteilung der Nachricht an weitere berechtigte Empfänger beim beA (dazu sogleich).
- Ein anderer Fall liegt vor, wenn auf eine E2EE zugunsten einer G2GE verzichtet wird, um den Perimeterschutz nicht zu gefährden. Denn wie das BSI ausführt, *„führt das Einbinden eines externen Dienstes mittels Ende-zu-Ende-Verschlüsselung […] in die lokale Sicherheitsinfrastruktur zu einem sicherheitstechnischen „Kurzschluss" des Perimeterschutzes".*[162] Unter diesem Aspekt kann im Ergebnis – je nach den gegebenen Risiken – der Verzicht auf E2EE unter Umständen auch zu einem Sicherheitsgewinn führen, wenn dadurch ein wirksamer Perimeterschutz (Firewall) gewährleistet wird.

---

161 Vgl. Durmus, DSB 2024, 236, 238.

162 BSI, Positionspapier Zero Trust 2023, S. 7.

5.1.5. Beispiele für (Verzicht auf) E2EE beim Transport sensibler Nachrichten

Es gibt mehrere Beispiele, in denen E2EE auch bei Nachrichten mit besonderem Schutzbedarf – nach den Umständen – nicht als rechtlich zwingend gebotene Maßnahme anzusehen ist bzw. bewusst andere Architekturentscheidungen getroffen wurden:

- E-Mail
    - Die DSK geht davon aus, dass E-Mail-Nachrichten mit hohem Schutzbedarf regelmäßig durch Ende-zu-Ende-Verschlüsselung (und zusätzlich eine qualifizierte Transportverschlüsselung) geschützt werden müssen. Sie stellen diese Forderung aber unter den Vorbehalt einer entsprechenden Risikoanalyse: *„Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese … verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.“*[163]
    - Das OLG Schleswig hat in einem Urteil eine Pflicht zur E2EE von E-Mails mit sensiblem Inhalt (Rechnung) aus der DSGVO abgeleitet;[164] diese Entscheidung wurde allerdings in der Literatur zu Recht kritisiert, da sie nicht berücksichtigt, dass bereits die Transportverschlüsselung nach dem Stand der Technik die relevanten Risiken hinreichend reduziert.[165] In weiteren Entscheidungen wurde für personenbezogene eine Verschlüsselung (ohne nähere Spezifizierung) als erforderlich angesehen;[166] dabei blieb jedoch offen, ob/wann nach Ansicht des Gerichts auch die strenge E2EE erforderlich ist.[167]
- Besonderes elektronisches Anwaltspostfach (beA)
    - Das besondere elektronische Anwaltspostfach wird für die Kommunikation der Rechtsanwälte mit Gerichten und Behörden von der Bundesrechtsanwaltskammer bereitgestellt (§ 31a BRAO). Nach § 20 Abs. 1 Satz 1 RAVPV ist es nach OSCI

---

[163] Vgl. DSK, Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Stand 16.06.2021, Ziffer 4.2.2.

[164] OLG Schleswig, Urt. v. 18.12.2024, Az. 12 U 9/24, juris Rn. 90 ff.

[165] Siehe Schuster, CR 2025, 184 ff.

[166] ArbG Suhl, Urt. v. 20.12.2023, Az. 6 Ca 704/23, juris Rn. 22.

[167] Dazu Sorber/Knoepffler, DSB 2024, 157, 158.

oder einem Nachfolgestandard zu betreiben. Es stellt einen „sicheren Übermittlungsweg“ im Sinne von § 130a Abs. 3 Satz 1 ZPO für die Kommunikation mit Zivilgerichten dar. Das beA arbeitet nicht mit einer echten E2EE. Es sieht vielmehr die technische Möglichkeit vor, dass im Rechenzentrum eine Umschlüsselung der Nachrichten vorgenommen werden kann, um eine Nachricht an andere, berechtigte Personen zu verteilen. Anders als beim OSCI-Standard vorgesehen, ist der verwendete öffentliche Schlüssel nicht der des tatsächlichen Empfängers/Postfachinhabers, sondern „nur“ der des Postfachs und befindet sich in der Obhut der das beA betreibenden BRAK.

  - Der Bundesgerichtshof (BGH) hat entschieden, dass diese Gestaltung rechtskonform ist und dass Rechtsanwälte keinen Anspruch darauf haben, dass das beA eine (echte) Ende-zu-Ende-Verschlüsselung bietet. Denn die einschlägigen Rechtsvorschriften verlangen keine E2EE. Die gesetzlichen Anforderungen „sicherer Übermittlungsweg“ und „sichere Kommunikation“ können auch auf anderem Weg erreicht werden und die einschlägigen Grundrechte verlangen keinen Schutz der Nachrichten durch E2EE.[168]

- De-Mail

  - Der Dienst „De-Mail“ soll einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr im Internet sicherstellen (§ 1 Abs. 1 De-Mail-Gesetz). Hierzu unterliegen De-Mail-Anbieter sehr strengen Anforderungen an die Gestaltung ihres Dienstes und die zu treffenden technisch-organisatorischen Maßnahmen. Dies Anforderungen sind durch das De-Mail-Gesetz vorgegeben und durch die BSI-Richtlinie TR 01201 konkretisiert. Nach diesen Vorgaben sind Nachrichten, die innerhalb des De-Mail-Verbundes versendet und empfangen werden, von den De-Mail-Anbietern obligatorisch auf Schadsoftware zu prüfen.[169]

---

168 BGH, Urt. v. 22.03.2021, Az. AnwZ (Brfg) 2/20, juris Rn. 50.

169 BSI, TR 01201 Teil 3.1, Version 1.8, Ziffer 3.1.1.1.

- Eine zentrale Prüfung auf Schadsoftware ist nur möglich, wenn die Nachricht nicht per E2EE verschlüsselt ist (daher ist die Prüfung auch nur dann vorgeschrieben).[170] Aus diesem Grund wurde bei der Konzeption von De-Mail bewusst auf die eigentlich wünschenswerte E2EE verzichtet – die Prüfbarkeit der Nachrichten auf Schadsoftware wurde in diesem Szenario als wichtiger angesehen. Allerdings sieht das Gesetz vor, dass die Teilnehmer sich freiwillig, außerhalb der technischen Funktionen von De-Mail, entscheiden können, ihre Nachricht Ende-zu-Ende zu verschlüsseln (§ 5 Abs. 3 Satz 3 De-Mail).

5.1.6. Anwendung auf Adapter

Wie gesehen sollte eine E2EE als hochgradig wirksame Schutzmaßnahme (zur Sicherstellung der Vertraulichkeit, aber auch Integrität und – bei Einsatz von PKI – Authentizität) bei der Planung und Maßnahmenauswahl hoch priorisiert werden. Alternativlos ist E2EE aber im Allgemeinen nicht. Sofern der Einsatz von Adaptern aus technischer Sicht nicht (oder nur mit besonders hohem Aufwand) verzichtbar ist und daher auf eine E2EE verzichtet werden soll, setzt dies voraus, dass hinreichende kompensierende TOM getroffen werden, die die Einhaltung der Schutzziele angemessen gewährleisten.

Bei der Auswahl kompensierender Maßnahmen sollten wiederum nach Möglichkeit Formen der Verschlüsselung gewählt werden, die einer E2EE möglichst nahekommen. So erreicht eine wirksame G2GE oder G2EE jedenfalls noch das Ziel, dass auf dem Weg der Nachricht über die zur Übertragung eingesetzten Dritten – also außerhalb der Netzwerke/Organisationen von Sender und Empfänger – ein Zugriff ausgeschlossen ist. Dies ist aus datenschutzrechtlicher Sicht grundsätzlich besser, als wenn der Adapter durch einen Dritten (Dienstleister) betrieben wird, der die Nachricht dann zumindest vorübergehend im Klartext innerhalb seines Hoheitsbereichs verarbeitet. Die Nachricht wird dann nicht mehr zwischen den Endnutzern, aber immerhin noch zwischen den verantwortlichen Stellen (z.B. Erkenntnisstelle und zuständiger Behörde) durchgehend verschlüsselt. Eine G2GE bzw. G2EE kann damit auch den oben genannten Vorteil erreichen, dass der Dienstleister im Sinne des Datenschutzes keine personenbezogenen Daten verarbeitet (1.2.2.2.). Dies setzt voraus, dass der Adapter im Hoheitsbereich des Senders (z.B. der

---

170 BSI, TR 01201 Teil 3.1, Version 1.8, Ziffer 3.1.1.1.

Erkenntnisstelle selbst) betrieben wird und nicht durch den OSiP-Anbieter. Diese wäre also, wenn keine E2EE gewählt wird, grundsätzlich zu bevorzugen.

5.2. Privacy by Design

Wie dargestellt, gilt E2EE als besonders relevante Maßnahme zur Einhaltung der Anforderungen an Privacy by Design.[171] Sie sollte daher Priorität bei der Planung erhalten und auf sie sollte nicht ohne triftige Begründung verzichtet werden. Unverzichtbar ist sie aber, wie bereits dargelegt, nicht (s.o.). Der Verzicht auf E2EE ist daher auch bei hohem Schutzbedarf bei entsprechender Begründung und hinreichenden kompensierenden Maßnahmen mit Privacy by Design vereinbar.

5.3. Zero Trust

Entsprechendes wie zu E2EE und Privacy by Design gilt auch für das Verhältnis von E2EE und Zero Trust. Beides sind im Ergebnis Sicherheitskonzepte, die sich ergänzen, aber nicht gegenseitig voraussetzen.

Zero Trust ist letztlich ein Zugriffs- und Identitätsmodell, das definiert, wer wann und wie auf welche Ressourcen zugreifen darf. Es trifft keine explizite Aussage über den Inhaltsschutz der Daten zwischen Endpunkten. Eine Zero-Trust-Architektur kann daher mit verschiedenen Verschlüsselungsansätzen betrieben werden, z.B. auch mit TLS auf Transportebene und mit Verschlüsselung im Ruhezustand.

Für eine technische Definition von Zero Trust kann auf die Publikation „Zero Trust Architecture" des NIST zurückgegriffen werden.[172] Danach gilt:

- Zero Trust beruht auf dem Kernprinzip „Never trust, always verify". Das bedeutet, dass kein Gerät oder Benutzer – ob innerhalb oder außerhalb des Netzwerks – automatisch als vertrauenswürdig eingestuft wird.
- Hieraus folgt u.a., dass es keine vertrauenswürdigen Zonen gibt und dass jede Verbindung zu verschlüsseln ist.[173]

---

171 Vgl. Durmus, DSB 2024, 236, 238.

172 NIST Special Publication 800-207, Zero Trust Architecture, August 2020, abrufbar unter: https://doi.org/10.6028/NIST.SP.800-207.

173 NIST Special Publication 800-207, Zero Trust Architecture, Ziffer 2.2 Nr. 1 (S. 8)..

- Es ergibt sich aber nicht zwingend, dass jegliche Kommunikation Ende-zu-Ende-verschlüsselt ist. Dies zeigt sich unter anderem daran, dass Zero Trust auch die Inspektion jeglichen Netzwerkverkehrs verlangt.[174] Dabei wird mit Blick auf die Inspizierbarkeit des Netzwerkverkehrs (Visibility on the Network) explizit davon ausgegangen, dass dieser ggf. (unaufbrechbar) verschlüsselt sein kann – dann sind Metadaten und Kommunikationsmuster zu analysieren – aber nicht notwendig (unaufbrechbar) verschlüsselt sein muss.[175] Im letzten Fall ist eine Deep Packet Inspection vorgeschrieben.

Das BSI beschreibt in seinem Positionspapier „Zero Trust" Anforderungen an eine „ideale" Verschlüsselung im Sinne von Zero Trust. Nach der Anforderung „NET-04" ist danach, jeder Netzwerkverkehr, innerhalb und außerhalb des Perimeters, zu verschlüsseln.[176] Bei der Verarbeitung von VS muss die Verarbeitung zwischen allen Geräten, die VS verarbeiten, zugelassen verschlüsselt sein (NET-VS).[177] Eine Ende-zu-Ende-Verschlüsselung wird dabei, soweit ersichtlich, aber gerade nicht verlangt.

5.4. Empfohlenes Betriebsmodell für Adapter

Aus den Ausführungen unter 5.1.6 ergibt sich, dass Adapter vorzugsweise innerhalb des Verantwortungsbereichs des Senders zu betreiben sind. Um die Argumentation zu ermöglichen, dass der Dienstleister keine (für ihn) personenbezogenen Daten verarbeitet, sollte dabei jegliche Zugriffsmöglichkeit durch den Dienstleister ausgeschlossen werden (1.2.2.2.). Im Falle von erforderlichen Wartungsarbeiten an dem vom Sender betriebenen Adapter sollte gleichwohl sicherheitshalber eine Auftragsverarbeitung vereinbart werden.

5.5. Persistieren von Daten in Adaptern

Ein Persistieren von Daten in Adaptern erscheint auf den ersten Blick als eine vermeidbare Verarbeitung, auf die schon unter dem Aspekt der Datenminimierung (und Speicherbegrenzung) nach Möglichkeit zu verzichten ist (Art. 5 DSGVO). Die Funktion der Adapter erscheint grundsätzlich einer flüchtigen Verarbeitung zu entsprechen. Sofern und solange aus technischen

---

174 NIST Special Publication 800-207, Zero Trust Architecture, Ziffer 3.4.1 Nr. 3 (S. 21): „The enterprise can observe all network traffic."

175 NIST Special Publication 800-207, Zero Trust Architecture, Ziffer 5.4, S. 28.

176 BSI, Positionspapier Zero Trust, 2023, S. 43.

177 BSI, Positionspapier Zero Trust, 2023, S. 43.

Gründen ein Persistieren erforderlich sein sollte, müsste dies in jedem Fall in verschlüsselter Form erfolgen. Eine solche Speicherung der Daten in Adaptern muss in die Risikoanalyse einbezogen und mit angemessenen TOM behandelt werden.

6. Rechtsgrundlagen für zentralen Betrieb?

Frage: „*Die meisten Anwendungsbereiche (z.B. Luftsicherheit) haben eine explizite Rechtsgrundlage. Die uns bekannten Rechtsgrundlagen sind im Anhang in einer Tabelle abgebildet. Erlauben diese Rechtsgrundlagen der FITKO den länderübergreifenden Betrieb?*"

Die aufgeführten Rechtsgrundlagen erlauben einen länderübergreifenden zentralen Betrieb durch die FITKO, sofern die fachliche Zuständigkeit der Landesbehörden unberührt bleibt und die gesetzlichen Verfahrens-, Trennungs- und Datenschutzregeln je Landesrecht systemseitig strikt umgesetzt werden.

Die Rechtsgrundlagen enthalten, soweit ersichtlich, keine ausdrückliche Regelung über den IT-Betrieb oder sonstige Regelungen, die einem länderübergreifenden Betrieb entgegenstehen.

Insbesondere die Sicherheitsüberprüfungsgesetze des Bundes und der Länder regeln Zuständigkeiten, Mitwirkungsstrukturen (Landesämter für Verfassungsschutz), Aktenführung sowie Datei-, Zweckbindungs- und Löschvorgaben näher. Sie enthalten jedoch, soweit ersichtlich, keine Pflicht zu einem landesindividuellen IT-Betrieb für das Fachverfahren zur Sicherheitsüberprüfung oder den verbundenen Datenaustausch. Die teils in den SÜG formulierte Anforderung, dass die im Rahmen einer ZSÜ verarbeiteten Daten nur an öffentliche Stellen übermittelt werden dürfen, steht nach der hier vertretenen Auffassung einer Auslagerung an einen (ggf. nichtöffentlichen) Auftragsverarbeiter nicht entgegen (siehe I.1.1.2.2.2.).

Allgemein müssen die aus den Rechtsgrundlagen ableitbaren technisch-organisatorischen Verfahrensvorgaben als Anforderungen an die OSiP-Anwendung aufgenommen und bei der Architektur berücksichtigt werden. Soweit ersichtlich, sind diese Vorgaben jedoch nicht ungewöhnlich und leiten sich in der Regel bereits aus allgemeinen Anforderungen des Datenschutzes (Art. 25, 32 DSGVO) und des IT-Grundschutzes ab und dürften demgemäß IT-technisch abbildbar sein. Beispiele für solche Anforderungen sind:

- In mehreren Ländern ist normiert, dass die Aufgaben der „zuständigen Stelle" innerhalb der Behörde organisatorisch von bestimmten anderen Aufgaben wie Personalrat oder Datenschutzbauftragtem zu trennen sind (etwa § 4 Abs. 1a BbgSÜG; § 4 Abs. 2 SÜG NRW). Hieraus ergibt sich, dass ein entsprechendes IT-Verfahren nicht nur mandantenfähig sein, sondern auch eine rollenbasierte Architektur aufweisen muss.
- Die länderspezifischen Datei-/Zweckbindungs-/Löschregime (u.a. §§ 19–23 SächsSÜG; §§ 19–23 LSÜG SH) und Sonderkapitel für nichtöffentliche Stellen (z.B. HmbSÜGG,

SiÜpG SL) sind durch parametrisierbare Retention-Engines, Empfänger-/Zweck-Whitelists, Protokollierung und dedizierte Tenants/Scopes technisch abbildbar.

- Ein rechtssicherer zentraler Betrieb setzt deshalb insbesondere voraus: klare Verantwortlichkeitszuordnung (Land als Verantwortliche; FITKO typischerweise als Auftragsverarbeiterin für Transport/Betrieb), strikte Mandantentrennung und Rechtekonzepte je Land/Behörde, VS-geeignete Be-triebs- und Zugriffskonzepte, länderspezifische Policy-Sets für Übermittlungen, Löschfristen und Akteneinsicht sowie revisionsfeste Protokoll- und Auskunftsfunktionen.

7. Rechtssichere Einwilligung

Frage: *„Bei den Anwendungsbereichen „Sicherheitsüberprüfung" und „anlassbezogene Überprüfungen" (siehe Datenschutzkonzept Seite 35.f) erfolgt die Überprüfung auf Basis einer unterschriebenen informierten Einwilligung der antragstellenden Person. Wie muss diese Einwilligung rechtssicher gestaltet werden? Kann eine einheitlich gestaltete Vorlage für alle Länder und den Bund verwendet werden?"*

Kurzantwort:

Die im Fachrecht zum Teil vorgeschriebene Zustimmung zur ZSÜ ist im Zweifel keine datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), aber gleichwohl eine Rechtmäßigkeitsvoraussetzung für die Durchführung der ZSÜ. Sie dient der Transparenz.

- Form: Es gibt föderale Divergenzen in den Formvorschriften (Schriftform vs. elektronische Form). Für die Fälle, wo echte Schriftform vorgeschrieben und eine Ersetzung durch die elektronische Form nicht zulässig ist, ist ein durchgängig medienbruchfreies Verfahren nicht umsetzbar.
- Inhalt: Inhaltlich ist zu beachten, dass die Zustimmung „informiert" erfolgen muss. Die zu erteilenden Informationen unterscheiden sich je nach Anwendungsfall: Rechtsgrundlage, Zweck, verarbeitete Daten, zuständigen Behörden und Erkenntnisstellen sind jeweils unterschiedlich. Eine vollständig einheitliche Vorlage müsste alle Fälle abdecken und erscheint daher unpraktikabel.

Empfohlenes Vorgehen:

1. Mustergestaltung: Die FITKO sollte ein allgemeines Template für die Zustimmung entwickeln (mit harmonisiertem Text und Platzhaltern für spezifische Informationen), das zugleich die datenschutzrechtlichen Transparenzanforderungen erfüllt. Aus diesem Template kann für jeden Anwendungsbereich eine Vorlage abgeleitet werden. Diese können die zuständigen Stellen eigenverantwortlich prüfen und übernehmen.
2. Form: Sofern die Zustimmung in OSiP verwaltet werden soll (insbesondere im Fachverfahren-Client), sollt für Anwendungsfälle mit zwingender Schriftform eine Upload-Möglichkeit vorgesehen werden. Im Übrigen kann die elektronische Form unterstützt werden, ggf. mit Möglichkeit zur elektronischen Signatur nach „eIDAS 2.0" (VO (EU) 2024/1183) (insbesondere im ggf. geplanten Antragsassistent nach OZG).

7.1. Zustimmungserfordernisse und Formanforderungen

Die unterschiedlichen Gesetze verlangen vor der Durchführung der Überprüfungen eine Einwilligung der betroffenen Person. Teilweise sind zusätzlich Einwilligungen der mitbetroffenen Person (z.B. Partner) erforderlich. Die Formvorgaben sind föderal unterschiedlich. Als Hintergrund ist zu berücksichtigen, dass eine gesetzliche vorgeschriebene Schriftform durch eine elektronische Form mit qualifizierter elektronischer Signatur ersetzt werden kann, sofern das die Schriftform anordnende Gesetz dies nicht ausdrücklich untersagt (§ 3a VwVfG). Damit ergibt sich:

Rechtsgrundlage	Einwilligung/Zustimmung erforderlich?	Form der Einwilligung/Zustimmung	Besonderheiten
Bund – SÜG (Bund)	Ja; Zustimmung ist Verfahrensvoraussetzung, Wortlaut in §§ 20 ff. implizit; Auskunfts-/Löschregime verweist auf „Einwilligung" für weitere Verarbeitung)	Die Zustimmung der betroffenen Person ist schriftlich oder nach Maßgabe von § 3a VwVfG oder unter Verwendung einer fortgeschrittenen elektronischen Signatur i.S.d. Art. 3 Nr. 11 eIDAS zu erteilen.	§ 23/§ 22 nennen Einwilligung (Auskunft/Verarbeitungseinschränkung); § 36 SÜG schränkt die entsprechende DSGVO-Geltung ein (nur selektive BDSG-Verweise).
Bund – Atomrecht (§ 12b AtG)	Ja (§ 12b Abs. 2 AtG)	Schriftlich (§ 12b Abs. 2 AtG); seit der Novellierung von 2009 ist die Ersetzung durch die (qualifizierte) elektronische Form nach § 3a VwVfG möglich (s. BT-Drs. 16/11709, S. 11).	-
Baden-Württemberg – SÜG BW	Ja (§ 2 Abs. 1 S. 2, § 2 Abs. 2 S. 3 LSÜG BW)	Schriftlich; die Sicherheitsüberprüfung bedarf der schriftlichen Zustimmung der betroffenen Person (§ 2 Abs. 1 S. 2 LSÜG BW). Auch für einbezogene Ehegatten/Lebenspartner ist die schriftliche Zustimmung erforderlich (§ 2 Abs. 2 S. 3 LSÜG BW).	Zustimmung der betroffenen Person ist ausdrückliche Verfahrensvoraussetzung; Schriftform für betroffene und mitbetroffene Person ausdrücklich im Gesetz geregelt; daneben detaillierte Regelungen zur Sicherheitserklärung, Datenverarbeitung und Löschung.
Bayern – BaySichPrüfG (BaySÜG)	Ja (Art. 4 Abs. 1 BaySÜG)	Schriftlich (Art. 4 Abs. 1 S. 2 BaySÜG)	Ausdrücklich Schriftform.

Berlin – SÜG BE	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 1 S. 1 SÜG BE)	Die Sicherheitserklärung ist schriftlich (vgl. § 7 Abs. 1 S. 2 SÜG BE). Eine ausdrückliche Formvorgabe für die Hauptzustimmung der betroffenen Person enthält das Gesetz nicht.	Zustimmung als Voraussetzung genannt; keine ausdrückliche Formvorgabe im Gesetzestext.
Brandenburg - BbgSÜG	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 1 S. 1 BbgSÜG)	Die Zustimmung der in § 8 Abs. 2 genannten Personen ist schriftlich oder elektronisch zu erteilen; bei schriftlicher Zustimmung genügt elektronische Übermittlung des Schriftstücks.	Lösch-/Speicherfortsetzung nur mit Zustimmung; Auskunft elektronisch/schriftlich möglich.
Bremen - BremSÜG	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 1 S. 1 BremSÜG)	Einwilligung schriftlich, elektronische Form ausgeschlossen (§ 7 Abs. 2 BremSÜG).	Elektronische Form ausgeschlossen (Bremer Norm fordert Schriftform für Zustimmung).
Hamburg - HmbSÜGG	Ja (§ 2 Abs. 1 S. 3–4, Abs. 2 S. 5–6 HmbSÜGG)	Zustimmung der betroffenen Person in Textform (§ 2 Abs. 1 S. 4 HmbSÜGG); Zustimmung der Partnerin/des Partners ebenfalls in Textform (§ 2 Abs. 2 S. 5–6 HmbSÜGG).	Zustimmung der betroffenen Person ist Verfahrensvoraussetzung; bei fehlender Zustimmung ist die Sicherheitsüberprüfung undurchführbar (§ 2 Abs. 3 HmbSÜGG). Einbeziehung der Partnerin/des Partners nur mit deren Zustimmung in Textform. Sicherheitserklärung mit detaillierten inhaltlichen Angaben in § 13 HmbSÜGG geregelt, ohne eigenständige Formvorgabe für die Erklärung selbst.
Hessen - HSÜVG	Ja (§ 2 Abs. 2, § 4 Abs. 1 HSÜVG)	Schriftlich für Sicherheitserklärung (§ 4 Abs. 1 S. 2 HSÜVG)	Schriftform vorgesehen (VO-spielräume bei Zuständigkeiten).
Mecklenburg-Vorpommern - SÜG M-V	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 1 S. 1 SÜG M-V)	Schriftlich für Sicherheitserklärung (§ 7 Abs. 1 S. 2); Schriftlich für mitbetroffene Person (§ 5 Abs. 5)	Hauptzustimmung ohne ausdrückliche Form; mitbetroffene Person: Schriftform. (Systematik wie in mehreren Ländern.)
Niedersachsen – Nds. SÜG	Ja (§ 5 Abs. 2 Nds. SÜG)	Schriftlich, sie kann nicht in elektronischer Form erteilt werden (§ 5 Abs. 2 Nds. SÜG)	„Die Einwilligung bedarf der Schriftform; sie kann nicht in elektronischer Form erteilt werden.“

Nordrhein-Westfalen – SÜG NRW	Ja (§ 7 Abs. 1 SÜG NRW)	Schriftlich; elektronische Form ausdrücklich ausgeschlossen (§ 8 Abs. 2 S. 3 SÜG NRW).	Einwilligung der betroffenen Person (und ggf. der mitbetroffenen Person) ist Verfahrensvoraussetzung; sie ist schriftlich zu erteilen, die elektronische Form ist ausdrücklich ausgeschlossen (§ 8 Abs. 2 S. 2–3 SÜG NRW).
Rheinland-Pfalz – LSÜG RP	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 1 S. 1 LSÜG RP)	Schriftlich (§ 8 Abs. 2 LSÜG RP)	Einwilligung der betroffenen Person als Verfahrensvoraussetzung; sie ist schriftlich, aber nicht in elektronischer Form zu erteilen (§ 8 Abs. 2 LSÜG RP)
Saarland - SSÜG	Ja (§ 2 Abs. 1, § 7 Abs. 1 SiÜpG)	Schriftlich (§ 2 Abs. 1 S. 3 SSÜG)	§ 2 Abs. 1/§ 16 (1): Zustimmung (betroffene Person und einbezogene Person) schriftlich; Altersgrenze 16.
Sachsen - SächsSÜG	Ja (§ 2 Abs. 2, § 7 Abs. 1 SächsSÜG)	-	Zustimmungserfordernis angelegt; keine explizite Form im Gesetzestext; Regelungen zur Sicherheitserklärung/mitbetroffene Person.
Schleswig-Holstein – LSÜG SH	Ja (§ 2 Abs. 1 S. 1, § 7 Abs. 2 LSÜG SH)	Schriftlich, nicht in elektronischer Form (§ 7 Abs. 2 und 5 LSÜG SH).	-
Thüringen - ThürSÜG	Ja (§ 6 Abs. 2 ThürSÜG)	-	Zustimmung als Voraussetzung normiert; keine Form ausdrücklich festgelegt.

Konsequenz: Ein bundesweit medienbruchfreies (durchgehend eSign-fähiges) Einwilligungsverfahren ist derzeit nicht flächendeckend zulässig. Mehrere Länder schließen in ihren SÜG die elektronische Form ausdrücklich aus (u.a. Niedersachsen, Schleswig-Holstein, Bremen, Nordrhein-Westfalen), während andere Länder und der Bund (zumindest für bestimmte Zustimmungen, etwa der mitbetroffenen Personen) elektronische Verfahren (teils mit fortgeschrittener e-Signatur) zulassen. Für ein Gesamtbild müssen zudem noch die Anwendungsfälle außerhalb der SÜG berücksichtigt werden. OSiP muss daher, um alle Anwendungsfälle abzubilden, technisch sowohl die Einholung und Dokumentation schriftlicher Einwilligungen (ggf. mit Scan/Upload)

als auch, soweit landes- oder bundesrechtlich zulässig, elektronischer Einwilligungen mit qualifizierter lektronischer Signatur (§ 3a VwVfG) unterstützen und diese je nach Rechtsgrundlage und Land konfigurierbar machen.

Hingegen ist die Anwendung des „Maximalprinzips" keine rechtlich zwingende und wohl auch keine zu empfehlende Konsequenz aus den heterogenen Formanforderungen. Maximalprinzip hieße, alle Zustimmungen schriftlich einzuholen. Das würde aber nicht berücksichtigen, dass in vielen Fällen der Gesetzgeber die elektronische Kommunikation im Überprüfungsverfahren bewusst zulassen wollte (und teilweise eigens durch Novellierung zugelassen hat, etwa in § 12b Abs. 2 AtG). Sinnvoller erscheint daher, die erforderlichen technischen Funktionen sowohl für Schriftform (also z.B. Upload als Scan zur Dokumentation, ggf. nach TR-RESISCAN) also auch für die elektronische und insbesondere die qualifizierte elektronische Form bereitzustellen und je nach Anwendungsfall die zulässigen Formen freizuschalten.

7.2. Rechtsnatur der Zustimmung

Die im Rahmen von Sicherheitsüberprüfungen verlangte „Zustimmung" ist ihrem Rechtscharakter nach keine datenschutzrechtliche Einwilligung im Sinne von Art. 6 Abs. 1 lit. a DSGVO, sondern eine fachrechtlich geforderte Mitwirkungs- bzw. Verfahrensvoraussetzung.[178]

Diese Zustimmung ist also Rechtsmäßigkeitsvoraussetzung für die ZSÜ, aber im Zweifel kein Erlaubnistatbestand für die Datenverarbeitung. Dieser ergibt sich vielmehr aus der jeweiligen Rechtsgrundlage für den OSiP-Anwendungsfall (I.1.1.1.3.1.). Nur außerhalb spezialgesetzlicher Ermächtigungen – etwa bei freiwilligen, anlassbezogenen Zutritts-/Akkreditierungsprüfungen ohne eine spezialgesetzliche Rechtsgrundlage kann die datenschutzrechtliche Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO im Einzelfall die tragende Rechtsgrundlage sein. Unabhängig davon ist zur Rechtssicherheit zu gewährleisten, dass eine vorgeschriebene Zustimmung tatsächlich vorliegt. Soweit dies in OSiP abgebildet werden soll – insbesondere in einem Fachverfahren-Client –, muss das System also vorsehen, dass eine formgerechte Zustimmung eingeholt wird.

[178] Vgl. Däubler, SÜG-Kommentar, 2019, § 2 Rn. 11 ff.

7.3. Voraussetzungen der Zustimmung

7.3.1. Informiertheit (Transparenz)

Die Zustimmung setzt eine vorherige, klare und verständliche Unterrichtung der betroffenen Person voraus. Diese muss den Zweck und die Rechtsgrundlagen der konkreten Überprüfung (einschließlich Überprüfungsart und -stufe sowie Zuständigkeiten), die Art und die Quellen der einzuholenden Auskünfte, die betroffenen Datenkategorien (einschließlich besonderer Kategorien), die Einbeziehung mitbetroffener Personen und deren gesonderte Zustimmung, die möglichen Folgen einer Verweigerung, die maßgeblichen Speicher-, Prüf- und Löschfristen einschließlich etwaiger Wiederholungs- oder Nachüberprüfungen sowie die Möglichkeit und die Wirkungen eines Widerrufs erläutern. Hinsichtlich des Inhalts ist der Transparenzinformation ist zu empfehlen, sich – soweit das Fachrecht keine besonderen Anforderungen stellt – an den Transparenzvorschriften der DSGVO zu orientieren (Art. 13/14 DSGVO). Die Unterrichtung ist zu dokumentieren, sollte also in den Zustimmungstext aufgenommen werden. Die Zustimmung muss sich erkennbar auf die konkret erläuterte Maßnahme beziehen und darf keine Blanko- oder Generaleinwilligung darstellen.

7.3.2. Bestimmtheit und Reichweite

Die Erklärung muss inhaltlich bestimmt sein. Sie hat die Überprüfungsart und -stufe, die zuständige Stelle, den zeitlichen Geltungsbereich einschließlich etwaiger Regel- oder Nachüberprüfungen sowie die einbezogenen Dritten konkret zu benennen. Teilweise oder einschränkende Zustimmungen sind zulässig, ihre Reichweite ist zu vermerken. Zugleich sind die möglichen Folgen begrenzter Mitwirkung – insbesondere die Undurchführbarkeit der Überprüfung – offen zu legen. Für mitbetroffene Personen ist stets eine separate, den gesetzlichen Vorgaben entsprechende Zustimmung einzuholen.

7.3.3. Form

Die Formvorgaben sind föderal uneinheitlich. Soweit das einschlägige Fachrecht Schriftform vorsieht, ist eine eigenhändige Namensunterschrift nach § 126 Abs. 1 BGB erforderlich. Die bloße Textform, etwa per E-Mail, genügt dann nicht. Einige Länder schließen die elektronische Form ausdrücklich aus, andere lassen qualifizierte elektronische Signaturen zu (hierfür gelten dann die Anforderungen der eIDAS-Verordnung in der geltenden Fassung (eIDAS 2.0“ (VO (EU)). Daraus folgt, dass ein bundesweit einheitlich rein elektronisches Einwilligungsverfahren

derzeit nicht flächendeckend rechtssicher umgesetzt werden kann und das Verfahren deshalb beide Varianten unterstützen sollte.

7.3.4. Freiwilligkeitsmaßstab und arbeits-/dienstrechtlicher Kontext

In der Regel wird die Zustimmung erteilt, weil andernfalls die weitere Laufbahn in Gefahr geraten oder bei einem Arbeitnehmer sogar die Kündigung drohen kann. Die Zustimmung ist daher regelmäßig nicht „freiwillig", bleibt aber fachrechtliche Verfahrensvoraussetzung.[179] Von einer „freiwilligen" Zustimmung kann höchstens die Rede sein, wenn ein Beschäftigter in eine gleichwertige nicht sicherheitsrelevante Tätigkeit ausweichen kann – was in der Praxis eher die Ausnahme sein wird.[180] Dies nimmt der Erklärung nicht ihren fachrechtlich geforderten Zustimmungscharakter, ersetzt aber auch nicht die – hier regelmäßig nicht einschlägige – datenschutzrechtliche Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO als Rechtsgrundlage der Verarbeitung. Soweit das Fachrecht auf Freiwilligkeitstatbestände bei Dritten verweist, etwa bei Referenzpersonen ohne dienst- oder arbeitsrechtliche Pflicht, ist auf die Freiwilligkeit ihrer Mitwirkung besonders hinzuweisen.

7.3.5. Persönliche Abgabe / Stellvertretung

Die Zustimmung ist höchstpersönlich abzugeben. Eine Stellvertretung scheidet wegen des Schutzes höchstpersönlicher Rechtsgüter aus. Bei Minderjährigen ist zu beachten, dass die Übertragung sicherheitsempfindlicher Tätigkeiten regelmäßig erst nach Vollendung des 16. Lebensjahres zulässig ist;[181] die Einleitung des Verfahrens kurz vor Erreichen dieser Altersgrenze kann erfolgen, um einen Einsatz ab 16 zu ermöglichen. Befindet sich die minderjährige Person in einem Arbeitsverhältnis, sind die arbeitsrechtlichen Zustimmungserfordernisse – insbesondere die Ermächtigung nach § 113 BGB – sicherzustellen, damit die/der Minderjährige wirksam selbst zustimmen kann. Auch insoweit sind aber ggf. die Besonderheiten des jeweiligen Fachrechts zu beachten.

---

[179] Vgl. Däubler, SÜG 2019, § 2, Rn. 11.

[180] Vgl. Däubler, SÜG 2019, § 2, Rn. 11.

[181] Vgl. Däubler, SÜG 2019, § 2, Rn. 15.

7.3.6. Zeitpunkt, Geltung und Widerruf

Die Zustimmung ist vor Beginn der Datenerhebung oder der Einholung von Auskünften einzuholen. Erweiterungen des Prüfprogramms, die vom ursprünglichen Zweck nicht gedeckt sind, bedürfen einer erneuten Zustimmung. Ein Widerruf ist jederzeit möglich und wirkt für die Zukunft; bereits vollzogene Verfahrensschritte bleiben unberührt. Der Widerruf kann die weitere Durchführung der Überprüfung unmöglich machen; der Umgang mit bereits erhobenen Daten richtet sich nach den gesetzlich normierten Lösch-, Sperr- und Aufbewahrungsregimen.

7.3.7. Dokumentation und Nachweis

Die zuständige Stelle hat die Zustimmung, die vorangegangene Unterrichtung, gegebenenfalls die Zustimmungen mitbetroffener Personen sowie Zeitpunkt und Form der Abgabe vollständig und nachvollziehbar zu dokumentieren. Die Aufbewahrungsdauer dieser Dokumentation richtet sich nach dem fachrechtlichen Akten- und Löschregime der sicherheitsüberprüfenden Stelle und ist entsprechend in das Verfahrensverzeichnis und die Löschkonzepte zu integrieren.

7.4. Empfohlene Umsetzung für OSiP – harmonisierte Muster

Aufgrund der divergierenden Formvorschriften und insbesondere der unterschiedlichen inhaltlichen Anforderungen an die Informiertheit der Zustimmung ist ein vollständig einheitliches Vorgehen nicht möglich.

Es ist zu empfehlen, ein einheitliches Template zu entwickeln, dass eine Struktur vorgibt, allgemeingültige Informationen (z.B. zum Einsatz von OSiP) enthält und im Übrigen Platzhalter für konkrete Informationen zum Verfahren und zur Datenverarbeitung im jeweiligen Anwendungsfall vorsieht. Daraus sollte dann für jeden OSiP-Anwendungsfall (z.B. Luftsicherheit, Atomrecht, Waffengesetz, anlassbezogene SÜ) ein eigenes, vollständig ausformuliertes Muster entwickelt werden. Dieses muss im Zweifel auch länder- bzw. bundesspezifisch ausgeprägt sein.

7.4.1. Struktur des Templates (und der abgeleiteten Muster)

Das Template kann aus zwei getrennten Bestandteilen aufgebaut sein, um Synergien zu nutzen und gleichzeitig die zwingenden rechtlichen Anforderungen zu erfüllen:

7.4.1.1. Harmonisierter Kerntext

Dieser Teil sollte harmonisierte Passagen enthalten. Er dient der Erfüllung der Transparenz- und Unterrichtungspflichten (Art. 13 ff. DSGVO) und kann zentral durch die FITKO bereitgestellt werden. Hierzu gehören:

- Verarbeitung durch OSiP: Allgemeine Beschreibung des Verfahrens
- Folgen der Verweigerung: Einheitliche Darstellung der rechtlichen Konsequenzen bei verweigerter Mitwirkung (z.B. Ausschluss von der Tätigkeit).
- Widerrufshinweise: Hinweise zu den rechtlichen Folgen des Widerrufs der Zustimmung

7.4.1.2. Spezifischer Teil (nach Anwendungsfall)

Dieser Teil muss durch spezifische Informationen ergänzt werden, da sie die Wirksamkeit der Zustimmung und die föderalen Besonderheiten abbilden:

- Zweck und Rechtsgrundlage
- Verarbeitete Daten
- Empfänger/Beteiligte (ggf. konkrete Nennung der Erkenntnisstellen)
- ggf. Löschfristen; Datenschutzinformationen (nach Art. 13 f. DSGVO oder dem sonst anwendbaren Datenschutzrecht)

7.4.1.3. Digitale Umsetzung

Die OSiP-Zielarchitektur muss die Zustimmungseinholung als dynamischen, hybriden Prozess abbilden, der die föderalen Formvorgaben technisch erzwingt.

7.4.1.3.1. Generierung und Bereitstellung des Dokuments

Die OSiP-Anwendung (z.B. der Frontoffice-Client) ist als Template-System zu konzipieren. Sie muss auf Basis der Nutzerangaben (Anwendungsbereich und zuständiges Bundesland) das korrekte, vollständig ausgefüllte Einzeldokument generieren und zum Download bereitstellen.

7.4.1.3.2. Medienbruchfreier/medienbruchbehafteter Prozess

Soweit das jeweilige Landesrecht strikt die Schriftform (§ 126 Abs. 1 BGB) verlangt, ist die Zustimmung analog einzuholen (Ausdruck und eigenhändige Unterschrift). Der Antragsteller muss das Dokument postalisch an die zuständige Genehmigungsbehörde versenden oder es – soweit

zulässig – digital (als Scan/Foto) hochladen. OSiP dient in diesem Fall als Gateway zur Übermittlung der Kopie.

Soweit die Formvorschriften des Landes die Textform (§ 126b BGB) oder die elektronische Form (§ 126a BGB) zulassen und das Verfahren dies technisch unterstützt, ist die digitale Einholung (z.B. durch einfache Bestätigung oder Qualifizierte Elektronische Signatur) ausreichend.

7.4.1.3.3. Systemseitige Validierung

Ist eine Zustimmung erforderlich und soll diese in OSiP verwaltet werden, so ist zu empfehlen, dass das OSiP-System die Bearbeitung des Antrags erst dann startet, wenn die Einhaltung der geforderten Form durch die zuständige Genehmigungsbehörde validiert wurde. Dies umfasst die Prüfung des Signaturstatus (bei QES) bzw. die Verifikation des physischen Originaldokuments (bei postalischem Eingang).

8. Regelung der Haftung bei Datenschutzverstößen

Frage: „*Wie sollte die Haftung für Datenschutzverstöße im Innenverhältnis zwischen der FITKO, dem zentralen Betreiber und den nutzenden Landesbehörden, insbesondere im Modell der gemeinsamen Verantwortlichkeit, vertraglich geregelt werden?*"

Kurzantwort:

Wir gehen davon aus, dass für den Betrieb das Modell der Auftragsverarbeitung angemessen ist und gewählt wird, also *nicht* das Modell der gemeinsamen Verantwortlichkeit (siehe 1.) Die Haftung gegenüber betroffenen Personen folgt in diesem Fall der gesamtschuldnerischen Außenhaftung nach Art. 82 Abs. 4 DSGVO. Im Innenverhältnis können die Beteiligten die Kosten- und Schadensverteilung vertraglich regeln (Art. 82 Abs. 5 DSGVO), sofern der vollständige Ersatzanspruch der betroffenen Person unberührt bleibt.

Aspekt	Juristische Basis / Empfehlung
Rollenmodell	FITKO ist Auftragsverarbeiterin (Art. 28 DSGVO). Der zentrale Betreiber ist Unterauftragsverarbeiter.
Außenhaftung FITKO	Im Außenverhältnis haften Verantwortliche und Auftragsverarbeiter gesamtschuldnerisch (Art. 82 Abs. 4 DSGVO). Die FITKO haftet nur, wenn sie eigene Pflichten der Auftragsverarbeitung verletzt oder rechtmäßige Weisungen missachtet (Art. 82 Abs. 2 S. 2 DSGVO); eine vollständige Exkulpation ist nach Art. 82 Abs. 3 DSGVO möglich, wenn sie „in keinerlei Hinsicht verantwortlich" ist.
Innenregress	Kausalitäts- und Verschuldensprinzip vertraglich festlegen (Art. 82 Abs. 5 DSGVO), ergänzt um klare Incident-Governance, Nachweis- und Mitwirkungspflichten sowie Kostenkatalog (Forensik, Benachrichtigung, Anwälte etc.).
Haftung für Unterauftragsverarbeiter	Nach Art. 28 Abs. 4 S. 2 DSGVO bleibt die Auftragsverarbeiterin gegenüber dem Verantwortlichen „voll verantwortlich" für die Erfüllung der Pflichten des Unterauftragsverarbeiters (strenge Einstandspflicht).
Bußgeldrisiko	Faktisch ausgeschlossen (§ 43 Abs. 3 BDSG), da FITKO als öffentliche Stelle gilt. Dasselbe gilt für die nutzenden öffentlichen Stellen.
Haftungs-Caps	Gegenüber Betroffenen unzulässig (Außenhaftung zwingend; Art. 82 DSGVO). Intern sind Cap-Regelungen für einfache Fahrlässigkeit grundsätzlich möglich, dürfen aber ErwGr. 146 / Art. 82 Abs. 5 nicht unterlaufen und müssen AGB-fest sein. Achtung: Caps dürfen die Einstandspflicht nach Art. 28 Abs. 4 S. 2 DSGVO gegenüber dem Verantwortlichen nicht faktisch aushöhlen (erhöhtes Unwirksamkeitsrisiko).

Dieser Abschnitt widmet sich der Haftungsverteilung im Innenverhältnis bei Datenschutzverstößen, welche primär durch Art. 82 DS-GVO und die vertraglichen Pflichten aus Art. 28 DS-GVO bestimmt wird. Ausgangspunkt der Analyse ist das präferierte Modell, in dem die nutzenden Landesbehörden die datenschutzrechtlich Verantwortlichen sind. Die FITKO erbringt Transport- und Plattformleistungen in der Rolle der Auftragsverarbeiterin nach Art. 28 DS-GVO, wobei der zentrale Betreiber als ihr Unterauftragsverarbeiter fungiert.

Die Haftungsrisiken für die FITKO manifestieren sich in diesem Modell in zwei Hauptbereichen: Zum einen drohen Schadensersatzansprüche betroffener Personen (Außenverhältnis), wenn diese materielle oder immaterielle Schäden[182] erleiden, die durch Pflichtverletzungen der FITKO – beispielsweise technische Mängel – verursacht wurden. Zum anderen ist die FITKO Regressansprüchen der Verantwortlichen (Innenverhältnis) ausgesetzt. Diese Regressforderungen zielen auf den Ersatz von Schäden ab, welche den Verantwortlichen aufgrund der Pflichtverletzung der FITKO im Rahmen der Auftragsverarbeitung entstanden sind. Solche Schäden umfassen insbesondere die vom Verantwortlichen bereits geleisteten Schadensersatzzahlungen an die betroffenen Personen nach Art. 82 DS-GVO.

8.1. Grundsatz: Gesamtschuldnerische Haftung im Außenverhältnis

Im Außenverhältnis gegenüber der betroffenen Person haften die Beteiligten an der Datenverarbeitung – der Verantwortliche und der Auftragsverarbeiter (wie die FITKO) – gemäß Art. 82 Abs. 4 DS-GVO grundsätzlich als Gesamtschuldner.[183] Anspruchsberechtigt ist jede unmittelbar betroffene natürliche Person der Verarbeitung (Art. 4 Nr. 1 DS-GVO). [184]

Sinn und Zweck der gesamtschuldnerischen Haftung ist es, dem Geschädigten einen wirksamen Ersatzanspruch zu gewährleisten (Erwägungsgrund 146). Demzufolge kann der Geschädigte jeden anspruchsverpflichteten Beteiligten nach seiner Wahl auf den gesamten ihm entstandenen Schaden in Anspruch nehmen, unabhängig davon, ob dieser den Schaden nur zu

---

[182] Vgl. zum Schadensbegriff Paal, MMR, 2020, 14, 16. Ein materieller Schaden kann etwa ein Datenverlust durch unberechtigte Weitergabe der Daten an unbefugte Dritte sein, die diese Daten missbrauchen (z.B. Missbrauch Kreditkarten- oder Bankdaten) und dadurch beim Betroffenen ein materieller Folgeschaden entsteht (Vermögensverlust).

[183] BeckOK DatenschutzR/Spoerr, 53. Ed. 1.8.2025, DS-GVO Art. 28, Rn. 44; Taeger/Gabel/Moos/Schefzig, 4. Aufl. 2022, DS-GVO Art. 82 Rn. 88 ff.

[184] Zur Frage, ob auch juristische Personen und nicht unmittelbar betroffene Personen anspruchsberechtigt sind, vgl. *Paal*, MMR 2020, 14 ff.

einem kleinen Teil verursacht hat. Die FITKO haftet deshalb in ihrer Rolle als Auftragsverarbeiterin unmittelbar und gesamtschuldnerisch, sofern sie an der Verarbeitung beteiligt war und sich nicht nach Maßgabe des Art. 82 Abs. 2 S. 2 und Abs. 3 DS-GVO erfolgreich exkulpieren kann.[185]

8.2. Haftungsprivilegierung des Auftragsverarbeiters

Während den Verantwortlichen nach Art. 82 Abs. 2 S. 1 DS-GVO die volle Haftung für die Einhaltung der gesetzlichen Vorschriften trifft, wird die FITKO als Auftragsverarbeiterin privilegiert und haftet gemäß Art. 82 Abs. 2 S. 2 DS-GVO gegenüber dem Betroffenen nur, wenn sie die ihr als Auftragsverarbeiterin nach der DS-GVO auferlegten Pflichten verletzt oder rechtmäßige Weisungen des Verantwortlichen missachtet.

8.3. Haftungsbefreiung des Auftragsverarbeiters

Sowohl der Verantwortliche als auch der Auftragsverarbeiter können von der Haftung gegenüber dem Betroffenen gemäß Art. 82 Abs. 3 DS-GVO befreit werden. Die FITKO als Auftragsverarbeiterin muss dazu nachweisen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, sie also kein „Verschulden" trifft.[186] Die FITKO als potenzielle Anspruchsgegnerin muss den Entlastungsbeweis nur für solche Verursachungsbeiträge führen, an denen sie beteiligt war. Im Übrigen genügt der Nachweis der fehlenden Beteiligung.[187]

8.4. Keine Haftungsbeschränkung im Außenverhältnis

Die FITKO kann die Haftung im Außenverhältnis gegenüber der betroffenen Person grundsätzlich nicht beschränken. Andernfalls würde die präventive Wirkung der Schadensersatzansprüche unterlaufen. Ein formularmäßiger Haftungsausschluss gegenüber Betroffenen hält in der Regel der Inhaltskontrolle des § 307 Abs. 2 Nr. 1 BGB nicht stand, da ein solcher Ausschluss der Haftung gegen das Leitbild des Art. 82 Abs. 1 DS-GVO verstoßen dürfte.[188]

---

[185] Kühling/Buchner/Hartung, 4. Auflage 2024, DS-GVO, Art. 28 Rn. 40; Paal, MMR 2020, 14, 18.

[186] „Verantwortlich" ist hier im Sinne des „Verschuldens" zu verstehen, vgl. Paal, MMR 2020, 14, 17.

[187] Paal, MMR 2020, 14, 17.

[188] Paal, MMR 2020, 14, 18.

8.5. Regressansprüche (Innenverhältnis)

Nachfolgend beleuchten wir den Gesamtschuldnerausgleich im Innenverhältnis zwischen den an der Datenverarbeitung Beteiligten, der sich primär nach Art. 82 Abs. 5 DS-GVO richtet und insoweit die Anwendung der allgemeinen nationalen Vorschrift des § 426 BGB überlagert. Die Aufteilung der Haftung erfolgt nach Maßgabe der jeweiligen Verantwortungsanteile der Schädiger. Für die Beurteilung des Beitrags der FITKO in ihrer Rolle als Auftragsverarbeiterin ist in diesem Ausgleich die Haftungsprivilegierung des Art. 82 Abs. 2 S. 2 DS-GVO von besonderer Bedeutung.

8.5.1. Zulässige Abreden im Innenverhältnis

Grundsätzlich können der Verantwortliche und die FITKO als Auftragsverarbeiterin im Innenverhältnis Haftungsbeschränkungen, Haftungsaufteilungen und Freistellungen vereinbaren. Die zwingende Voraussetzung für die Zulässigkeit dieser internen Abreden ist jedoch, dass sie den vollständigen und wirksamen Ersatzanspruch der betroffenen Person im Außenverhältnis nicht gefährden (vgl. Erwägungsgrund 146 S. 6). Eine solche Gefährdung würde die präventive Funktion der Schadensersatzansprüche, die alle Beteiligten zu datenschutzrechtskonformem Handeln motivieren soll, unterlaufen. Die Aufnahme von Freistellungsvereinbarungen zugunsten der FITKO ist insbesondere dann sinnvoll, wenn die zugrundeliegende Pflichtverletzung allein in den Verantwortungsbereich des Verantwortlichen fällt. Solche Abreden werden typischerweise im Vertrag zur Auftragsverarbeitung (AVV) getroffen.

8.5.2. Haftung des Auftragsverarbeiters für Unterauftragsverarbeiter

Die Inanspruchnahme von Unterauftragsverarbeitern verschärft die Haftungslage des Auftragsverarbeiters. Gemäß Art. 28 Abs. 4 S. 2 DS-GVO haftet die FITKO als Auftragsverarbeiterin gegenüber der verantwortlichen Behörde verschuldensunabhängig für die Pflichtverstöße ihres Unterauftragsverarbeiters. Diese gesetzliche Garantiehaftung besteht allein im Innenverhältnis zum Verantwortlichen. Gegenüber betroffenen Personen im Außenverhältnis kann sich die FITKO weiterhin nach Maßgabe des Art. 82 Abs. 3 DS-GVO exkulpieren.

Die Frage, ob die FITKO im Innenverhältnis mit dem Verantwortlichen die verschuldensunabhängige Haftung für Verstöße des Unterauftragsverarbeiters vertraglich beschränken kann, ist unklar. Zwar enthält die DS-GVO – anders als etwa § 14 ProdHaftG – kein explizites Unabdingbarkeitsgebot. Daher spricht die Privatautonomie grundsätzlich für die Zulässigkeit einer Haftungsbeschränkung in einer frei verhandelten Individualvereinbarung.

Allerdings spricht der klare Zuweisungscharakter des Art. 28 Abs. 4 S. 2 DS-GVO gegen eine Abdingbarkeit, da die Norm eine spezifische Garantiehaftung des Auftragsverarbeiters gegenüber dem Verantwortlichen statuiert. Eine vertragliche Einschränkung birgt daher das Risiko der Unwirksamkeit wegen Verstoßes gegen den Grundgedanken dieser spezifischen Haftungszuweisung. Zudem ist zu beachten, dass die Regelung des Art. 28 Abs. 4 S. 2 DS-GVO nur die Haftung für den Unterauftragsverarbeiter, nicht jedoch die Haftung des Auftragsverarbeiters für seine eigenen Verstöße betrifft, für die der Innenausgleich nach Art. 82 Abs. 5 DS-GVO gilt. Finden auf die Vereinbarung die AGB-Inhaltskontrolle Anwendung, sind die Beschränkungsmöglichkeiten ohnehin stark eingeschränkt (§§ 307 ff. BGB).

Im Falle einer Inanspruchnahme durch den Verantwortlichen steht der FITKO stets eine Regressmöglichkeit gegenüber dem Unterauftragsverarbeiter zu, der den Verstoß kausal verursacht hat. Unabhängig von der vertraglichen Ausgestaltung dürfte ein Anspruch auf Schadensersatz gegen den Unterauftragsverarbeiter wegen der Verletzung seiner Pflichten aus dem Auftragsverarbeitungsvertrag bereits nach den allgemeinen Grundsätzen der §§ 280 ff. BGB bestehen. Ergänzend dazu sollte die Aufnahme einer expliziten vertraglichen Freistellungsverpflichtung im Unterauftragsverarbeitungsvertrag erwogen werden, um die Geltendmachung des Regresses zu vereinfachen und abzusichern.

8.6. Faktisch kein Bußgeldrisiko nach Art. 83 DS-GVO

Ein faktisches Risiko für die FITKO, selbst Bußgelder wegen Datenschutzverstößen auferlegt zu bekommen, oder Bußgelder im Wege des Regresses gegenüber den Verantwortlichen zu erstatten, sehen wir nicht.

Die Datenschutz-Grundverordnung räumt den Mitgliedstaaten in Art. 83 Abs. 7 DS-GVO eine Öffnungsklausel ein, um die Sanktionierung öffentlicher Stellen durch Geldbußen national zu regeln oder auszuschließen. Der deutsche Gesetzgeber hat diese Befugnis in § 43 Abs. 3 BDSG dahingehend umgesetzt, dass gegen Behörden und sonstige öffentliche Stellen des Bundes grundsätzlich keine Bußgelder verhängt werden, wobei öffentliche Stellen des Bundes auch Anstalten des öffentlichen Rechts umfassen (§ 2 Abs. 1 BDSG). Vergleichbare Regelungen finden sich auch in den jeweiligen Landesdatenschutzgesetzen, so dass eine Verhängung von Bußgeldern auch gegenüber Landesbehörden nicht erfolgen wird.[189]

[189] Vgl. z.B. § 24 Abs. 3 HmbDSG, Art. 23 Abs. 2 BayDSG.

Die FITKO ist eine länderübergreifende Anstalt des öffentlichen Rechts (§ 5 IT-StV), die in gemeinsamer Trägerschaft von Bund und Ländern steht (§ 6 Abs. 1 IT-StV). § 43 Abs. 3 BDSG Bundesstellen verweist zwar nur auf Behörden und öffentliche Stellen des Bundes, das für die FITKO gemäß § 6 Abs. 3 S. 1 IT-StV anwendbare Hessische Datenschutz- und Informationsfreiheitsgesetz enthält jedoch in § 36 Abs. 2 HDSIG eine entsprechende Regelung.

Diese Privilegierung gilt allerdings nur, solange die öffentliche Stelle hoheitlich oder im Rahmen ihrer öffentlichen Zweckbestimmung handelt. Öffentliche Stellen, die als Unternehmen am Wettbewerb teilnehmen, sind gemäß § 2 Abs. 5 BDSG als nicht-öffentliche Stellen zu behandeln und damit bußgeldpflichtig. Im vorliegenden Fall des OSiP-Projekts liegt jedoch kein Wettbewerbshandeln vor. Für die nutzenden Stellen handelt es sich um die hoheitliche Aufgabe der Durchführung (bzw. seitens der Erkenntnisstellen der Unterstützung) gesetzlich vorgeschriebener ZSÜ. Für die FITKO handelt es sich um die öffentliche Aufgabe der Unterstützung dieser Tätigkeit (insbesondere da OSiP mit Haushaltsmitteln finanziert und für andere öffentliche Stellen entwickelt wird).

Aber selbst wenn gegen einen Verantwortlichen ein Bußgeld verhängt werden sollte, ist fraglich, ob der Verantwortliche das Bußgeld von der FITKO im Wege des Regresses ersetzt verlangen kann. Denn ein Bußgeld (z.B. nach Art. 83 DS-GVO) stellt in der Regel keinen „Schaden" dar, sondern eine öffentliche Sanktion des Staates oder der Aufsichtsbehörde zur Abschreckung und Ahndung. Kann der Täter das Bußgeld oder die Geldstrafe von einem Dritten zurückverlangen, kann dies allerdings die Sanktionswirkung beeinträchtigen. Daher stellen Geldstrafen und Geldbußen grundsätzlich keinen ersatzfähigen Schaden dar.[190]

[190] Näher hierzu BeckOK IT-Recht/Hilber, 19. Ed. 1.4.2025, BGB § 249 Rn. 15 ff. auch mit Ausführungen zur Ansicht des EuGH, nach dem jedenfalls unter Gesamtschuldnern im Innenverhältnis eine privatautonome Regressregelung bzgl. eines Bußgeldes getroffen werden könne, ohne dass dies dem Sanktionszweck von Bußgeldern entgegenstünde.

III. Netzinfrastruktur und Zugangswege

1. Zulässige Netze für OSiP

Frage: *„In welchen Netzen darf, bzw. muss das Produkt OSiP betrieben werden (z.B. Landesverwaltungsnetze, Polizei- oder Justiznetze)?"*

Kurzantwort:

Der Datenaustausch von OSiP zwischen Bund und Ländern ist gemäß § 3 Abs. 1 IT-NetzG zwingend über das Verbindungsnetz durchzuführen.

Die OSiP-Infrastruktur (Transportinfrastruktur, Backend) muss daher unmittelbar an das Verbindungsnetz angeschlossen sein.

Aspekt	Anforderung	Konsequenz für den Betreiber
Anschlusszwang	§ 3 Abs. 1 IT-NetzG verpflichtet zum Austausch über das Verbindungsnetz. Eine Ausnahme gilt nur für OZG-Dienste – also für einen der OSiP-Antragsdienst für Bürger/Unternehmen –, nicht für den Transportdienst.	Die FITKO (bzw. ihr beauftragter Betreiber) muss einen direkten Anschluss an das Verbindungsnetz oder die angeschlossenen Netze der Länder besitzen.
Sicherheitsniveau	Die Anschlussbedingungen (IT-PLR-Beschluss 2020/15) verlangen hohe IT-Sicherheitsstandards.	Der Betreiber ist vertraglich auf die Einhaltung des IT-Grundschutzes und der Anschlussbedingungen verpflichtet (i.d.R. nachgewiesen durch das Profil „Verbindungsnetz Teilnehmer-Anschluss [VN TNA]").
Zertifizierung	Erforderlich ist in der Regel eine Zertifizierung ISO 27001 auf Basis von IT-Grundschutz mit dem Geltungsbereich des VN TNA-Anschlusses.	Zertifizierungsanforderung

1.1. Verbindungsnetz

1.1.1. Pflicht zum Datenaustausch über das Verbindungsnetz (§ 3 IT-NetzG)

Eine wesentliche Funktion von OSiP ist die Ermöglichung eines ebenenübergreifenden Datenaustausches zwischen den für die Zuverlässigkeits- und Sicherheitsüberprüfung zuständigen Stellen und den Erkenntnisstellen. Ein solcher Datenaustausch zwischen den Beteiligten Stellen des Bundes und der Länder ist nach § 3 Abs. 1 Satz 1 IT-NetzG ausschließlich über das Verbindungsnetz durchzuführen. Ziel dieser Vorgabe ist es laut Gesetzesbegründung, *„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“*.[191]

Eine Ausnahme von der Verpflichtung zur Nutzung des Verbindungsnetzes ist nur für den Anwendungsbereich des Onlinezugangsgesetzes vorgesehen (§ 3 Abs. 1 Satz 2 IT-NetzG), der auch über andere Netze des Bundes (NdB) mit entsprechendem IT-Sicherheitsstandard erfolgen darf. Diese Ausnahme gilt jedoch nur für einen evtl. OSiP-Onlinedienst, also einen Dienst, der Bürgern oder Unternehmen die Online-Antragstellung auf Durchführung einer Zuverlässigkeits- oder Sicherheitsüberprüfung ermöglicht. Nur diese Komponente wäre ein Onlinedienst gem. § 2 Nr. 8 OZG und damit vom Anschlusszwang an das Verbindungsnetz ausgenommen. Für die übrigen OSiP-Komponenten, wie etwa für den Transportdienst, den FO-Client und den Erkenntnisstellen-Client, bleibt es bei der Pflicht zur Nutzung des Verbindungsnetzes.

Die Verpflichtung zur Nutzung des Verbindungsnetzes nach § 3 Abs. 1 Satz 1 IT-NetzG betrifft nur den Datenaustausch. Diesbezüglich gelten die verbindlichen Vorgaben durch das IT-NetzG und das zuständige Kontrollgremium, den IT-Planungsrat (§ 4 IT-NetzG). Die Kompetenzen für die an das Verbindungsnetz angeschlossenen Bundes- und Landesnetze verbleiben beim Bund bzw. dem jeweiligen Land.[192]

---

191 BT-Drs. 16/12400, S. 23.

192 BT-Drs. 16/12400, S. 23.

1.1.2. Anschluss der OSiP-Nutzer

Alle Landesnetze und die relevanten sonstigen öffentlichen Netze sind bereits an das Verbindungsnetz angeschlossen. Es ist also davon auszugehen, dass für die OSiP nutzenden öffentlichen Stellen die Voraussetzungen für einen Datenaustausch gemäß § 3 Abs. 1 Satz 1 IT-NetzG bereits vorliegen.

1.1.3. Anschluss des OSiP-Betreibers

Da im derzeitigen Zielbild über die OSiP-Infrastruktur (nämlich über den Server für das Frontend, das Backend und insbesondere über die Transportinfrastruktur) Daten zwischen Bund und Ländern ausgetauscht werden und ein solcher Austausch über das Verbindungsnetz erfolgen muss, muss wegen § 3 Abs. 1 Satz 1 IT-NetzG auch der Betreiber der OSiP-Infrastruktur an das Verbindungsnetz angeschlossen sein.

Der Betreiber kann durch einen eigenständigen, direkten Anschluss an das Verbindungsnetz angeschlossen sein. Die Ausgestaltung von § 3 IT-NetzG durch die Beschlüsse des IT-Planungsrats und das Konzept der IVÖV sehen vor, dass IT-Dienstleister unmittelbar an das Verbindungsnetz angeschlossen werden können, ohne dass dieser Anschluss über ein Landesnetz oder ein sonstiges Netz vermittelt werden muss.

Ein direkt an das Verbindungsnetz angeschlossener IT-Dienstleister (OSiP-Betreiber) muss die unter 1.1.4 genannten sicherheitstechnischen Vorgaben erfüllen. Er müsste also sein Rechenzentrum (oder einen Teil davon) als hochsichere Zone betreiben und dort die OSiP-Infrastruktur aufbauen. Dies gilt mindestens für die OSiP-Transportinfrastruktur, da diese den Datenaustausch zwischen den nutzenden Stellen vermittelt.

1.1.4. Vorgaben für den Anschluss an das Verbindungsnetz

Technische Vorgaben für den Anschluss an das Verbindungsnetz ergeben sich aus:

- den Anschlussbedingungen für das Verbindungsnetz, Version 2.0, beschlossen mit IT-PLR-Beschluss 2020/15[193];

[193] https://www.it-planungsrat.de/beschluss/beschluss-2020-15 (die eigentlichen Anschlussbedingungen als Anlage sind auf der Seite des IT-PLR nicht veröffentlicht).

- dem Leistungskatalog für das NdB-Verbindungsnetz, Version 2.9, beschlossen mit IT-PLR-Beschluss 2024/29[194];
- der Leistungsvereinbarung (vgl. Leistungsvereinbarung Bundeseinrichtungen, beschlossen mit IT-PLR-Beschluss 2022-53)[195];
- dem IT-Grundschutzprofil „Verbindungsnetz Teilnehmer-Anschluss (VN TNA)", welches nach den Anschlussbedingungen durch die Teilnehmer einzuhalten ist.[196]

Der Betreiber ist, soweit anwendbar, gesetzlich nach § 8 BSIG auf die Einhaltung der Mindeststandards des BSI und den IT-Grundschutz verpflichtet. Jedenfalls muss er zur Teilnahme am Verbindungsnetz die „Anschluss- und Nutzungsbedingungen (ANB) der BDBOS" abschließen und ist darüber vertraglich auf den IT-Grundschutz verpflichtet.

Der Betreiber muss in der Regel ein Zertifikat nach „ISO 27001 auf der Basis von IT-Grundschutz" nachweisen. Hierfür müssen seine Prozesse, Rechenzentren und die Netzarchitektur entsprechend hohe Sicherheitsanforderungen (z.B. zu Netzsegmentierung, Firewalling, VPNs) erfüllen.

1.2. Vorgaben für Netzübergänge

Nach der föderalen IT-Architekturrichtlinie, TV-09 Kommunikation, Regel Nr. 1 *soll* die Kommunikation *„über zentral bereitgestellte gesicherte Netze, Netzanschlüsse, Netzzugänge, Netzkopplungen und Netzübergänge erfolgen (u.a. IVÖV, KTN)"*.[197]

Nach Regel Nr. 3 *muss* die Kommunikation „innerhalb der definierten Netzzonen (u.a. Grundschutz, Hoch) oder entlang des Sicherheitsgefälles" erfolgen.

---

194 https://www.it-planungsrat.de/fileadmin/beschluesse/2024/Beschluss2024-29_Verbindungsnetz_Teilnehmerpreise_Leistungskatalog.pdf.

195 https://www.it-planungsrat.de/fileadmin/beschluesse/2022/Beschluss2022-53_Leistungsvereinbarung.pdf.

196 Zahlreiche öffentliche IT-Dienstleister verfügen über entsprechende Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz mit dem Geltungsbereich „Verbindungsnetz Teilnehmeranschluss (VN TNA)", z.B. das ITZBund, die BITBW in Baden-Württemberg oder die HZD in Hessen).

197 IT-Architekturrichtlinie, V1.9.0, TV-09 Kommunikation, S. 54.

1.3. Geheimschutz (VS-NfD)

Das Verbindungsnetz selbst genügt dem Schutzbedarf „hoch" und ist für die Übertragung von VS-NfD-eingestuften Daten nach VSA-Bund geeignet. Die von der Betreiberin, der BDBOS, eingesetzten Kryptoendgeräte sind vom BSI für den Geheimhaltungsgrad VS-NfD zugelassen.

Die Anschlussbedingungen verlangen, dass, sofern tatsächlich VS-NfD-eingestufte Daten von den Teilnehmern übertragen werden, die Teilnehmer sicherstellen, dass die gesamte Kommunikationsstrecke Ende-zu-Ende für VS-NfD geeignet ist.[198] Dazu muss die OSiP-Transportinfrastruktur die Anforderungen an VS-IT nach der VSA erfüllen und für das gesamte Verfahren muss, da es sich um VS-IT handelt, der BSI-Baustein „CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)" modelliert werden (siehe I.1.3.).

[198] VN-NdB, Leistungskatalog v2.9, Ziffer 5.1.1.

2. Zulässigkeit eines Cloud-Betriebs

Frage: *„Ist ein Betrieb in einer privatwirtschaftlichen Cloud-Infrastruktur bei einem zentralen Betriebsmodell rechtlich zulässig? Wenn dies zulässig ist, welche technischen und organisatorischen Maßnahmen müssten hierfür zusätzlich getroffen werden?"*

Kurzantwort:

Rein datenschutzrechtlich betrachtet könnte ein zentral betriebener OSiP-Dienst grundsätzlich in einer privatwirtschaftlichen Cloud-Infrastruktur betrieben werden. Die bereits benannten zwingenden technischen und vertragliche Mindestanforderungen sind dabei einzuhalten:

Anforderung	Rechtliche Grundlage	Konsequenz für den Betrieb
Netzanbindung	§ 3 IT-NetzG und Netzstrategie 2030.	Der Zugriff muss ausschließlich über das Verbindungsnetz oder ein gleichwertig gesichertes Bundesnetz erfolgen (keine direkten Internetpfade).
Digitale Souveränität	FAR (AV-09) und DVC-Strategie.	Die Verwaltung muss die technische und vertragliche Steuerungs- und Exit-Fähigkeit behalten (Vermeidung von Lock-in-Effekten).
Informationssicherheit	Art. 32 DSGVO und BSI-Mindeststandards NIS2-VO	Der Betreiber muss die Einhaltung durch ein C5:2020-Testat (oder vergleichbare BSI-Zertifikate) nachweisen; Hoheit über Kryptografische Schlüssel muss bei der Verwaltung liegen. Ferner muss der Anbieter die KRITIS-Anforderungen (NIS2-VO) erfüllen.
Drittlandtransfer	Kapitel V DSGVO	Es sollte eine zwingende Lokalisierung innerhalb der EU/EWR vereinbart werden. Zugriffe aus Drittländern müssten technisch unterbunden oder durch geeignete Garantien abgesichert werden (Art. 44 ff. DSGVO).

Im Falle der Einbeziehung einer privatwirtschaftlichen Cloud-Infrastruktur erhält das Ziel einer E2EE-Verschlüsselung zusätzliche Priorität und kann ggf. sogar als zwingende Vorgabe zur

Risikobehandlung aus den vorzunehmenden Risikobetrachtungen etwa nach Art. 32 DSGVO abzuleiten sein.

Ferner ist mit Blick auf das Leitbild der nationalen digitalen Souveränität ist angesichts der hohen Kritikalität von OSiP zu empfehlen, den Betrieb auf Deutschland zu beschränken (II.1.4.1.).

2.1. Kein datenschutzrechtlicher Ausschluss privatrechtlicher Betreiber

Rein datenschutzrechtlich ist die Auslagerung einer Datenverarbeitung durch privatrechtliche Betreiber im Zusammenhang mit den OSiP-Anwendungsfällen nicht ausgeschlossen.

Soweit in den Rechtsgrundlagen für die ZSÜ zum Teil die Übertragung von Daten an nicht-öffentliche Stellen ausgeschlossen wird, sprechen überwiegende Gründe dafür, dass dies zwar einer Übermittlung an nicht-öffentliche Stellen als Verantwortliche, aber nicht einer Weitergabe an einen nicht-öffentlichen Auftragsverarbeiter entgegensteht. Allerdings empfiehlt sich zur Rechtssicherheit dann in besonderem Maße für die Inhaltsdaten eine E2EE (s.o. I.3.2.).

Soweit Art. 10 DSGVO vorsieht, dass die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten „nur unter behördlicher Aufsicht" vorgenommen werden darf oder soweit dies nach dem EU-Recht oder nationalem Recht zugelassen ist, steht auch dies der Beauftragung eines privatwirtschaftlichen Dienstleisters nicht entgegen. Eine entsprechende Aufsicht liegt vor, wenn eine Behörde für die Verarbeitung verantwortlich ist und die nicht-öffentliche verarbeitende Stelle als Auftragsverarbeiter gebunden ist.[199] Auch insoweit ergibt sich aber sicherheitshalber erst Recht die Empfehlung, in einem solchen Fall eine E2EE-Verschlüsselung vorzusehen und somit einen Zugriff auf kritische inhaltliche Daten für den Betreiber und auf das Transportstrecke insgesamt von vornherein auszuschließen.

2.2. Netz- und Zuständigkeitsrahmen

Der Datenaustausch zwischen Bund und Ländern hat über das Verbindungsnetz zu erfolgen (siehe 1.1). Diese Voraussetzung muss auch bei einem Cloud-Betrieb gewahrt werden, steht diesem aber nicht prinzipiell entgegen. Cloud-basierte Dienste privater Anbieter dürfen also eingebunden werden, sofern der Zugriff über das Verbindungsnetz geführt wird.

---

[199] Vgl. Petri in Simitis/Hornung/Spiecker gen. Döhmann, 2. Aufl., Art. 10 DSGVO Rn. 18.

Bei der Einbindung eines privaten Cloud-Anbieters muss dieser hohe Sicherheitsstandards erfüllen. Diese ergeben sich bereits aus den Anschlussbedingungen für das Verbindungsnetz und im Übrigen aus den anwendbaren Datenschutz- und IT-Sicherheitsbestimmungen.

2.3. Digitale Souveränität als verbindliche Leitplanke

Die Netzstrategie 2030 formuliert ein Souveränitätsziel:[200] Für die Netzinfrastruktur der öffentlichen Verwaltung wird ein Eigenbetriebsmodell mit internem Netzdienstleister und nationalem Routing verfolgt. Externe Cloud-Ressourcen dürfen daran anknüpfen, wenn die Netzherrschaft der Verwaltung gewahrt bleibt und der Verkehr entsprechend den Vorgaben des Bundesnetzes geführt wird.

Die Föderale IT-Architekturrichtlinie (FAR v1.9.0) macht „Digitale Souveränität" zur allgemeinen Vorgabe (AV-09).[201] Danach müssen Lösungen kontrollierbar und steuerbar sein, Wechselmöglichkeiten bieten und durch ausreichende interne Kompetenzen abgesichert werden. Eine privatwirtschaftliche Cloud ist damit vereinbar, wenn die Verwaltung technische und vertragliche Steuerungs- und Exit-Rechte behält und ihre Wechsel- und Portabilitätsfähigkeit nachweisbar ist.

Aktuelle Beschlüsse zur Deutschen Verwaltungscloud (DVC) zeigen die zulässige Ausgestaltung in der Praxis: Cloud-Services sollen über ein föderales Cloud-Service-Portal angeboten werden. Neben öffentlichen IT-Dienstleistern können perspektivisch auch verwaltungsexterne Anbieter beteiligt werden, allerdings nur nach DVC-Konformitätsstandards und unter föderaler Gesamtsteuerung durch FITKO.[202] Das bestätigt die grundsätzliche Zulässigkeit privater Clouds, wenn die Souveränitäts- und Sicherheitsvorgaben eingehalten werden.

---

[200] Vgl. Netzstrategie 2030 für die öffentliche Verwaltung, S. 9.

[201] Vgl. Föderale IT-Architekturrichtlinie, Version 1.9.0, AV-09 „Digitale Souveränität" (Kontrollierbarkeit/Steuerbarkeit, Wechselmöglichkeiten, interne Kompetenzen), IT-Planungsrat, Beschluss 2025/17, 2025.

[202] Vgl. Deutsche Verwaltungscloud (DVC): Abschlussbericht Umsetzungsprojekt (08.04.2025); Produkt-/Zielarchitektur-Unterlagen (Cloud-Service-Portal, Konformitätskriterien, Einbindung externer Anbieter) sowie Protokoll 46. IT-Planungsratssitzung (26.03.2025).

Mit Blick auf das Ziel der nationalen digitalen Souveränität und des „Nationalen Routings“ (Netzstrategie 2030) und der hohen Kritikalität von OSiP ist zu empfehlen, diesen Rahmentscheidungen bei der Planung hohe Priorität einzuräumen und als Leistungsort Deutschland anzunehmen (s.o. II.1.4.1.).

2.4. Datenschutzrechtlicher Rahmen

Die Wahl der Betriebsumgebung ändert nichts an den grundsätzlichen Pflichten aus der DSGVO, ist aber bei der Risikoanalyse und ggf. zu treffenden Maßnahmen zu berücksichtigen (Art. 28, 32 DSGVO). Eine privatwirtschaftliche Cloud oder ein Betrieb außerhalb Deutschlands führt zu erhöhten Risiken, die durch TOM abgebildet werden müssen (z.B. durch E2EE).

Sobald eine Auslagerung mit Datenzugriffen in ein Drittland verbunden wäre, sind zusätzlich die Anforderungen aus Kapitel V (Art. 44 ff. DSGVO) einzuhalten, etwa über einen Angemessenheitsbeschluss oder geeignete Garantien wie Standardvertragsklauseln, ergänzt um technische Schutzmaßnahmen, die ein gleichwertiges Schutzniveau herstellen. Zu empfehlen ist eine Drittlandübermittlung mit Blick auf das Leitbild der Nationalen Digitalen Souveränität für OSiP jedoch – wie gesagt – nicht, sondern vielmehr eine Beschränkung auf den Verarbeitungsort Deutschland (Nationales Routing).

2.5. Informationssicherheit: Mindeststandards und Prüfregime

Für die Bundesverwaltung gelten die BSI-Mindeststandards „Nutzung externer Cloud-Dienste“ als verbindliches Mindestniveau. Sie verlangen u.a. eine Cloud-Strategie, ein systematisches Risikomanagement, klare Rollen- und Verantwortlichkeiten, Betriebs- und Exit-Konzepte, Logging/Monitoring sowie Anforderungen an Verschlüsselung, Identitäts- und Zugriffsmanagement.[203] Als marktübliche Nachweislinie hat sich das BSI-C5-Prüfverfahren etabliert, das von unabhängigen Auditoren testiert wird und international an ISO/IEC-Standards andockt; die jeweils aktuelle Fassung ist C5:2020.[204] Für Länder und Kommunen sind die Mindeststandards nicht unmittelbar verpflichtend, dienen aber als maßgebliche Orientierung.[205]

---

[203] Vgl. BSI-Mindeststandard „Nutzung externer Cloud-Dienste“, Version 2.1 (15.12.2022).

[204] Vgl. BSI „Cloud Computing Compliance Criteria Catalogue – C5:2020“ (aktuelle Fassung), Bundesamt für Sicherheit in der Informationstechnik.

[205] Vgl. BSI, „Antworten auf häufig gestellte Fragen zu den Mindeststandards“ (FAQ), Frage „Auf wen finden die Mindeststandards Anwendung?“, link: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/FAQ_MST/faq_mst_node.html.

2.6. Zusätzliche TOM für private Clouds

Die folgenden TOM erscheinen aus datenschutzrechtlicher Sicht (insbesondere) bei einer privatwirtschaftlichen Cloud – soweit technisch für das Verfahren geeignet – geboten bzw. zu empfehlen:

2.6.1. Netz- und Zugriffsarchitektur

Die Cloud-Umgebung ist über das Verbindungsnetz anzubinden, sodass keine Internetpfade für Verwaltungszwecke genutzt werden. Der Netzverkehr wird segmentiert und nach dem Zero-Trust-Prinzip abgesichert. Für den Zugriff sind ein föderationsfähiges Identitäts- und Rechtemanagement, das Prinzip minimaler Rechte sowie ein privilegiertes Zugriffsmanagement umzusetzen. Sämtliche sicherheitsrelevanten Ereignisse werden lückenlos protokolliert, zentral korreliert und dauerhaft auswertbar gemacht.

2.6.2. Kryptografie und Datenhoheit

Sämtliche Daten werden nach dem Stand der Technik während der Übertragung und im Ruhezustand verschlüsselt. Die Verwaltung behält die alleinige Hoheit über kryptografische Schlüssel oder nutzt eine kundenseitige Schlüsselverwaltung mit Hardware-Sicherheitsmodulen und dokumentierten Rotationsplänen (bzw. einem Schlüsselmanagement entsprechend den Anforderungen des BSI).

Die Datenlokalisierung sollte innerhalb der EU beziehungsweise des EWR erfolgen, bzw. mit Blick auf das Ziel der digitalen nationalen Souveränität und des nationalen Routings bei einem kritische Verfahren wie OSiP in Deutschland. Soweit aus technischen oder supportbedingten Gründen potenzielle Zugriffe aus Drittländern nicht vollständig ausgeschlossen werden können, sind diese technisch zu unterbinden oder durch zusätzliche Schutzmaßnahmen im Einklang mit der DSGVO zu kontrollieren (Art. 44 ff. DSGVO).

2.6.3. Betriebs- und Nachweisregime

Der Anbieter weist ein etabliertes Informationssicherheitsniveau durch einschlägige Prüfberichte und Zertifizierungen nach und hält diese in regelmäßigen Abständen aktuell. Auf Seiten der Verwaltung liegt eine Cloud-Strategie mit Risikobehandlungsplan, Notfall- und Wiederanlaufkonzept, dokumentierter Backup-Strategie einschließlich Unveränderbarkeit sowie regel-

mäßig getesteten Wiederherstellungsübungen vor. Das Betriebsmodell stellt ein kontinuierliches Monitoring, eine klare Störungs- und Incident-Prozesskette sowie eine rechtskonforme Protokollierung sicher.

2.6.4. Souveränitäts- und Exit-Fähigkeit

Die Verwaltung wahrt ihre digitale Souveränität durch vertraglich abgesicherte Steuerungsrechte. Dazu gehören umfassende Audit- und Kontrollrechte, definierte Informations- und Berichtspflichten, Portabilitäts- und Wechselmechanismen ohne unzumutbare Abhängigkeiten sowie ein verbindlicher Exit-Plan mit Fristen, Formaten und Unterstützungsleistungen des Anbieters. Datenrückgabe, sichere Löschung und Nachweispflichten sind präzise geregelt, und Schnittstellen sowie Datenformate sind so gewählt, dass ein Anbieterwechsel technisch praktikabel bleibt.

2.6.5. Rollen, Verantwortlichkeiten und Datenschutz

Die Rollenverteilung wird eindeutig festgelegt, in der Regel in Form einer Auftragsverarbeitung mit klar geregelten Unterauftragsbeziehungen und Genehmigungsmechanismen. Der Vertrag enthält einen vollständigen Maßnahmenkatalog zu Identitäts- und Zugriffsmanagement, Protokollierung, Schwachstellenmanagement, Patch- und Change-Prozessen sowie eine verbindliche Incident-Governance mit Meldewegen und Fristen. Für Verarbeitungsvorgänge mit erhöhtem Risiko wird eine Datenschutz-Folgenabschätzung durchgeführt; Übermittlungen in Drittländer werden nur unter Einhaltung der Anforderungen der DSGVO zugelassen.

2.6.6. Einbettung in die föderale Cloud-Landschaft

Um einen geprüften rechtlichen Rahmen zu nutzen, ist zu überlegen, den Dienst so zu gestalten, dass er sich in die föderale Cloud-Governance einfügt und die dort definierten Konformitätskriterien erfüllt. Dies umfasst die Nutzung offener Standards und Schnittstellen, eine konsistente Metadaten- und Katalogisierungspraxis sowie die Fähigkeit, über ein gemeinsames Cloud-Service-Portal verwaltet zu werden. Gleichzeitig werden Wiederverwendung, Interoperabilität und eine abgestimmte Gesamtsteuerung sichergestellt, damit Betrieb, Sicherheit und Souveränität über föderale Ebenen hinweg konsistent bleiben.

2.7. Ergebnis

Ein zentral betriebener OSiP-Dienst kann rechtssicher in einer privatwirtschaftlichen Cloud laufen, wenn die Netzanbindung über das Verbindungsnetz erfolgt, die DSGVO einschließlich Kapitel V eingehalten wird und die Leitplanken „Digitale Souveränität“ aus Netzstrategie 2030 und FAR umgesetzt sind. In der Praxis sollte die Vergabe zwingend BSI-Mindeststandards für externe Cloud-Dienste und ein C5-Testat voraussetzen, vertraglich die Exit- und Audit-Fähigkeit absichern. Zu überlegen ist, die Einbindung in die DVC-Governance vorzusehen, um gemeinsame Mechanismen für Sicherheit, Rechtmäßigkeit und föderale Steuerbarkeit zu nutzen.

3. Betrieb und Zugang über das Internet

Frage: *„Gibt es Vorgaben, die den Betrieb und den Zugang über das Internet einschränken?"*

Kurzantwort:

Ja. OSiP ist nicht lediglich ein ausgelagertes IT- bzw. Fachverfahren, sondern ein Verfahren zum Datenaustausch zwischen Bund und Ländern. Hierfür ist das Verbindungsnetz vorgeschrieben. Ein Betrieb oder Zugang über das Internet (womit letztlich auch der Datenaustausch über das Internet geführt würde) ist damit grundsätzlich nicht vereinbar und würde dem Sinn der Anbindung über das Verbindungsnetz widersprechen. So müssen auch die seitens eines technischen Betreibers an das Verbindungsnetz angebundenen Bereich, in denen OSiP-Infrastruktur steht, vom Internet hinreichend technisch getrennt sein.

Ob hiervon in bestimmten begrenzten Fällen – etwa bei der Kommunikation mit Dritten, die nicht unter das IT-NetzG fällt – abgewichen werden kann, müsste im Einzelfall geprüft werden.

Für den OZG-Antragsdienst ist hingegen eine Anbindung zum Bürger/Antragsteller über das Internet bzw. den Portalverbund möglich und vorgesehen. Der OZG-Dienst ist aber vom eigentlichen OSiP-Dienst (Frontend/Backend/Fachverfahren, Transportinfratruktur) zu trennen.

Unabhängig davon gilt allgemein:

Die „Netzstrategie 2030" und die Föderale IT-Architekturrichtlinie statuieren Leitplanken zur digitalen Souveränität (u.a. nationales Routing, Steuerbarkeit, Exit-Fähigkeit). Bei Internet-Zugriffen sind die BSI-Vorgaben (ISi-Reihe, IT-Grundschutz, TR-02102 Krypto, Mindeststandard Cloud und C5-Nachweise) einzuhalten. Für Verschlusssachen gelten darüber hinaus besonders strenge Vorgaben; eine Nutzung offener Netze ist nur unter BSI-zugelassenen Krypto-Maßnahmen und Freigaben zulässig. Diese Rahmenbedingungen schränken den Betrieb „über das Internet" ein und verlangen technische Gegenmaßnahmen (z.B. abgesicherte Gateways, VPN/Zero-Trust, starke Kryptografie) und organisatorische Steuerungsrechte.

3.1. Verbindungsnetz statt „offenes Internet" als Regelweg

Der Datenaustausch zwischen Bund und Ländern hat über das Verbindungsnetz zu erfolgen.

Im OZG-Anwendungsbereich darf er ausnahmsweise auch über andere Netze des Bundes erfolgen, *sofern* dort ein dem beabsichtigten Datenaustausch entsprechender IT-Sicherheitsstandard nachgewiesen wird. Diese Ausnahme betrifft aber im Fall von OSiP lediglich den OZG-Antragsdienst.

Im Übrigen gilt allgemein:

3.2. Nationales Routing und Steuerbarkeit

Die Netzstrategie 2030 formuliert „nationale digitale Souveränität" als Ziel und sieht hierfür ein Eigenbetriebsmodell mit internem Netzdienstleister und nationalem Routing vor. Internet-Anbindungen zentraler Dienste müssen sich daran ausrichten (z.B. Führung des Verkehrs über das Bundesnetz, keine unnötigen Auslandsrouten). Die Föderale IT-Architekturrichtlinie (FAR) V1.9.0 macht „Digitale Souveränität" zur allgemeinen Vorgabe (AV-09) und verlangt Kontrollierbarkeit/Steuerbarkeit, Austauschbarkeit/Wechselmöglichkeiten und ausreichende interne Kompetenzen. Diese Vorgaben begrenzen die operative Abhängigkeit von reinen Internet-Zugängen und verlangen steuerbare, auditierbare und exit-fähige Anbindungen.

3.3. Sicherheitsanforderungen für Internetzugänge der Verwaltung

Das BSI fordert für Internet-Zugriffe abgesicherte Zugangswege (Security-Gateway/DMZ, Segmentierung, Least-Privilege, Protokollierung) und bei Fernzugriffen kryptographisch gesicherte VPNs bzw. Zero-Trust-Prinzipien. Die ISi-Reihe (u.a. „Sicherer Fernzugriff auf das interne Netz") und begleitende Veröffentlichungen definieren hierfür Mindestmaßnahmen; die Technische Richtlinie TR-02102 legt den Stand der Technik für Algorithmen und Schlüssellängen fest. Diese Vorgaben erlauben Internet-Zugriffe, schränken sie aber in der Ausgestaltung stark ein (z.B. verpflichtende starke Kryptografie, Gateways, Monitoring).

3.4. Cloud-Bezug: Mindeststandard „Externe Cloud-Dienste" und C5

Wenn zentrale Komponenten oder Randdienste über das Internet auf Cloud-Ressourcen zugreifen, gelten für die Bundesverwaltung der BSI-Mindeststandard „Nutzung externer Cloud-Dienste" (Governance, IAM, Verschlüsselung, Logging/Monitoring, Exit-Konzepte) und als Prüfnachweis das BSI-C5:2020-Attest. Für Länder/Kommunen sind diese Mindeststandards nicht unmittelbar verpflichtend, werden aber regelmäßig als Orientierung/Maßstab verlangt. Dadurch ergeben sich indirekte Beschränkungen für Internet-Zugänge (z.B. nur freigeschaltete

Schnittstellen, verpflichtende Transport-sowie Ruhend-Verschlüsselung, Nachweis- und Auditpflichten).

3.5. Höhere Schutzbedarfe und Verschlusssachen

Sobald Verschlusssachen (VS) betroffen sind, greifen die Verschlusssachenanweisungen des Bundes bzw. der Länder. Danach ist die Übertragung über offene Netze nur unter behördlich zugelassenen, BSI-freigegebenen Krypto-Verfahren/-Produkten und nach Freigabe des Informationssicherheitsbeauftragten zulässig; in vielen Fällen sind gesonderte, VS-zugelassene Netze erforderlich. Das schränkt Internet-Nutzungen für diese Datenkategorien deutlich ein.

3.6. Praktische Konsequenz für zentrale Fachverfahren

Für Behördenzugriffe auf zentrale Dienste (z.B. OSiP-Backoffice) ist Internet-Zugang nur über gesicherte, geprüfte Pfade (Verbindungsnetz/gleichwertiges Bundesnetz plus Gateway/VPN/Zero-Trust) einzurichten. Bürger-Portale dürfen über das Internet erreichbar sein, müssen jedoch gemäß BSI-Vorgaben hinter sicheren Web-Bereitstellungen (z.B. DMZ, WAF/Reverse-Proxy, Härtung, Monitoring, sichere Krypto nach TR-02102) betrieben werden. Für Cloud-Anbindungen sind Mindeststandard-Kontrollen und C5-Nachweise einzufordern; bei VS-Bezug sind öffentliche Netze nur ausnahmsweise und mit VS-zugelassenen Maßnahmen zulässig.

IV. Betreiberanforderungen

1. Vorgaben für Auswahl/Beauftragung Betreiber

Frage: *„Welche rechtlichen Vorgaben, insbesondere aus Datenschutzsicht (z.B. Datenübermittlung ins außereuropäische Ausland), gelten für die Auswahl und Beauftragung eines zentralen Betreibers?"*

Kurzantwort:

Die Auswahl des Betreibers (als Unterauftragsverarbeiter) erfordert den Nachweis hinreichender Garantien für die Einhaltung der datenschutzrechtlichen Bestimmungen (Art. 28 Abs. 1 DSGVO). In der Praxis erfolgt dies durch Zertifizierungen und ggf. Audits. Die zu fordernden Garantien sollten die Bereiche Datenlokation und ISMS/Risikomanagement/TOM (einschließlich Netzanbindung) abdecken. Zu fordern sind BSI-konforme Zertifizierungen (ISO/IT-Grundschutz, C5-Testat) und – aufgrund der Anforderungen der NIS2-Umsetzung – der Nachweis der Einhaltung der KRITIS-Vorgaben.

Aufgrund der besonderen Anforderungen erscheint es jedoch geboten, sich in diesem Fall nicht lediglich auf die Vorlage von Zertifizierungen zu beschränken, sondern das gesamte Sicherheitskonzept – soweit für OSiP relevant – detailliert zu prüfen. Die Prüfung muss außerdem in festzulegenden, gebotenen Abständen wiederholt werden.

Der Vertrag muss einen Auftragsverarbeitungsvertrag (AVV nach Art. 28 Abs. 3 DSGVO) enthalten, der die Pflichten über die gesamte Kette spiegelt. Drittlandsübermittlungen sind aus den bereits genannten Gründen zu vermeiden, müssten aber aus Datenschutzsicht jedenfalls zwingend den Anforderungen der Art. 44 ff. DSGVO genügen. Zu empfehlen ist aber, wie bereits gesagt, eine Festlegung auf den Verarbeitungsort Deutschland.

1.1. Datenschutzrechtliche Sorgfaltspflichten (Art. 28 DSGVO)

1.1.1. Nachweis der „Hinreichenden Garantien"

Die FITKO – als Auftragsverarbeiterin der Länder – muss nach Art. 28 Abs. 1 DSGVO gewährleisten, dass der eingesetzte zentrale Betreiber (Sub-Auftragsverarbeiter) hinreichende Garantien für die Einhaltung des Datenschutzes bietet. Dies ist die juristische Pflicht zur Sorgfaltsprüfung (Due Diligence). Maßgebliche Nachweise der Eignung sind:

- **Zertifizierungen (ISMS-Basis):** Nachweis eines wirksamen Informationssicherheits-Managementsystems (ISMS), belegt durch eine Zertifizierung nach ISO/IEC 27001 auf Basis von BSI-IT-Grundschutz. Dieses sollte auch die besonderen Anforderungen des NIS2-VO (KRITIS) umsetzen.
- **Cloud-Sicherheit:** Bei Cloud-Nutzung die Vorlage eines aktuellen BSI-C5:2020-Prüfattests (oder gleichwertig).
- **Konzept:** Vorhandensein von belastbaren Rollen- und Rechtemodellen, Exit-/Reversibilitätskonzepten sowie integrierten Incident- und Monitoring-Prozessen.

Aufgrund der besonderen Anforderungen erscheint es geboten, sich in diesem Fall nicht lediglich auf die Vorlage von Zertifizierungen zu beschränken, sondern das gesamte Sicherheitskonzept – soweit für OSiP relevant – detailliert und individuell zu prüfen. Der Nachweis bzw. die Prüfung müssen außerdem in festzulegenden, gebotenen Abständen wiederholt werden.

1.1.2. Vertragswerk (Auftragsverarbeitung)

Die Zusammenarbeit ist durch einen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 Abs. 3 DSGVO abzusichern. Der Vertrag muss die Pflichten der FITKO an den Unterauftragsverarbeiter spiegeln und umfassende Kontroll- und Auditrechte der FITKO bzw. der Länder sichern.

1.2. Spezifische Anforderungen an Lokation und Netz (Digitale Souveränität)

1.2.1. Drittlandübermittlung und Datenlokation (Kapitel V DSGVO)

Eine Übermittlung personenbezogener Daten an einen Betreiber in einem außereuropäischen Ausland (Drittland) oder die Möglichkeit des Drittlandzugriffs sollte aus Datenschutzsicht mit Blick auf das Risikoprofil von OSiP unbedingt vermieden werden. Die Datenlokation sollte nach Möglichkeit auf Deutschland beschränkt werden (s.o. zur nationalen digitalen Souveränität).

Sollte ein Drittlandtransfer gleichwohl unvermeidbar erscheinen (etwa aufgrund globaler Supportstrukturen), sind jedenfalls die hohen Anforderungen aus Kapitel V DSGVO (Art. 44 ff. DSGVO) einzuhalten. Dies erfordert zusätzlich zu Transfermechanismen wie den Standardvertragsklauseln technische Schutzmaßnahmen (z.B. kundenseitige Schlüsselhoheit, Verschlüsselung im Ruhezustand), um ein geleichwertiges Schutzniveau zu gewährleisten. Zu empfehlen ist eine solche Konstruktion jedoch im Fall von OSiP nicht.

1.2.2. Netzanbindung und Souveränität

Die Vorgaben des IT-NetzG und die strategischen Ziele des IT-Planungsrats sind vertraglich durchzusetzen:

- Anschlusszwang: Der Betreiber muss die Einhaltung des Anschlusszwangs gewährleisten. Der Datenaustausch des OSiP-Transportdienstes muss ausschließlich über das Verbindungsnetz erfolgen (§ 3 Abs. 1 IT-NetzG)) oder ein gleichwertig gesichertes Verwaltungsnetz.
- Sicherheitsniveau: Der Betreiber muss den Sicherheitsstandard "hoch" und das IT-Grundschutzprofil „Verbindungsnetz Teilnehmer-Anschluss (VN TNA)“ nachweisen sowie die Einhaltung der Vorgaben der NIS2-VO.
- Digitale Souveränität: Die Verpflichtungen aus der Föderalen IT-Architekturrichtlinie (FAR) und der Netzstrategie 2030 sind zu integrieren. Dies umfasst vertraglich abgesicherte Steuerungs-, Portabilitäts- und Exit-Rechte der Verwaltung, um sogenannte "Vendor-Lock-ins" zu vermeiden.

1.3. Organisations- und Vergaberechtliche Pflichten

Die Informationssicherheits-Leitlinie des IT-Planungsrats verlangt, dass der Auftragnehmer vertraglich auf die verbindlichen Vorgaben der Leitlinie verpflichtet und kontrolliert wird (Informationssicherheits-Leitlinie 2018, Ziffer 5). Die Auswahl und Beauftragung des Betreibers muss im Übrigen die allgemeinen Vergaberechtsvorschriften beachten.

2. Erforderliche Zertifizierungen des Betreibers

Frage: *„Welche Zertifizierungen sind für die Betreiber erforderlich (z.B. ISO 27001)?"*

Kurzantwort:

Erforderlich ist regelmäßig (1) ein nachweislich wirksames ISMS mit ISO/IEC 27001-Zertifikat auf der Basis von BSI-IT-Grundschutz im jeweils relevanten Geltungsbereich und (2) – bei Cloud-Bezug – ein aktuelles BSI-C5:2020-Prüfattest als marktüblicher Nachweis der Cloud-Kontrollen. Für die Teilnahme am Verbindungsnetz sind das IT-Grundschutz-Profil „VN-TNA" und hierfür ISO 27001 auf Basis IT-Grundschutz maßgeblich. Schließlich sollte der Anbieter geeignete Testate erbringen, dass sein ISMS den Anforderungen der NIS2-VO genügt.

2.1. ISMS und BSI-IT-Grundschutz

Für den Betrieb von IT-Systemen der öffentlichen Verwaltung ist ein etabliertes Informationssicherheits-Managementsystem (ISMS) nachzuweisen. Der Betreiber muss ein ISO/IEC 27001-Zertifikat vorlegen, welches den internationalen Standard für das ISMS belegt. Präferiert wird jedoch die Zertifizierung ISO 27001 auf der Basis von BSI-IT-Grundschutz. Diese verbindet den prozessorientierten Ansatz der ISO-Norm mit den detaillierten, maßnahmenorientierten Vorgaben des BSI-IT-Grundschutz-Kompendiums. Dies ist für den öffentlichen Sektor der robustere Nachweis der Angemessenheit der TOM.

2.2. Anforderungen für den Anschluss an das Verbindungsnetz

Da der OSiP-Transportdienst dem Anschlusszwang (§ 3 IT-NetzG) unterliegt, muss der Betreiber die hierfür geltenden, erhöhten Sicherheitsstandards nachweisen:

- Vertragliche Pflicht: Es müssen die Anschluss- und Nutzungsbedingungen (ANB) der BDBOS vertraglich akzeptiert werden.
- IT-Grundschutzprofil: Zwingend einzuhalten ist das IT-Grundschutz-Profil „Verbindungsnetz Teilnehmer-Anschluss (VN TNA)". Dies Profil definiert die konkreten Maßnahmen, die am Übergang des Rechenzentrums zum Verbindungsnetz erforderlich sind.
- Nachweis: Die Einhaltung des VN-TNA-Profils wird in der Praxis durch das ISO 27001 auf Basis IT-Grundschutz-Zertifikat mit dem Geltungsbereich „VN-TNA-Anschluss" belegt. Ohne diesen Nachweis kann der sichere Netzbetrieb nicht belegt werden.

2.3. Cloud-Bezug – Mindeststandard und C5-Testat

Soweit zentrale OSiP-Komponenten in einer Cloud-Infrastruktur (IaaS/PaaS/SaaS) betrieben werden, gelten zusätzliche Anforderungen:

- Mindeststandard: Für die Bundesverwaltung ist die Einhaltung des BSI-Mindeststandards „Nutzung externer Cloud-Dienste“ verbindlich und gilt für Länder und Kommunen als maßgeblicher Orientierungsrahmen.
- Marktnachweis: Der Nachweis der Einhaltung der Cloud-Kontrollen erfolgt durch das BSI-C5:2020-Prüfattest. Obwohl das C5-Attest kein „Zertifikat“ im engeren Sinne ist, wird es als gleichwertiger, transparenter Eignungs- und Prüfnachweis in öffentlichen Ausschreibungen regelmäßig gefordert.

2.4. Ergebnis und Vertragsgestaltung

Der Betreiber ist vertraglich zur Vorlage folgender Nachweise zu verpflichten:

- ISO/IEC 27001 auf Basi IT-Grundschutz (mit dem Geltungsbereich des VN-TNA-Anschlusses)
- Aktuelles BSI-C5:2020-Prüfattest (bei Cloud-Benutzung).
- Diese Zertifizierungen stellen die Grundlage für die Einhaltung der Technischen und Organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO und die vertraglich abzusichernden Audit-Rechte dar.

3. Verantwortungs- und Haftungsfragen FITKO/Betreiber

Frage: „*Welche Verantwortlichkeiten und Haftungsfragen ergeben sich aus dem zentralen Betrieb für das FITKO-Produktmanagement und den Betreiber der Software?*"

Kurzantwort:

Die fachlich entscheidenden Landesbehörden sind datenschutzrechtlich Verantwortliche. Die FITKO erbringt Transport-/Plattformleistungen als Auftragsverarbeiterin (Art. 28 DSGVO). Der zentrale Betreiber agiert als Unterauftragsverarbeiter der FITKO. Gegenüber betroffenen Personen gilt die gesamtschuldnerische Außenhaftung nach Art. 82 DSGVO. Auftragsverarbeiter haften jedoch nur bei Verletzung eigener AV-Pflichten oder bei Missachtung rechtmäßiger Weisungen und können sich nach Art. 82 Abs. 3 DSGVO exkulpieren. Im Innenverhältnis ist eine vertragliche Regressordnung nach Kausalität/Verschulden festzulegen (inkl. Incident-Governance und Kostenkatalog). Für Unteraufträge bleibt die FITKO der verantwortlichen Behörde gegenüber voll verantwortlich (Art. 28 Abs. 4 S. 2 DSGVO). Bußgelder gegen die FITKO sind als öffentliche Stelle regelmäßig ausgeschlossen (nationale Regelung), ohne dass dies die zivilrechtliche Außenhaftung berührt. Vgl. zum Rollenmodell und den Netz-/Sicherheitsanforderungen die Abschnitte II.1 und III.1.

3.1. Verantwortlichkeiten (Rollen und Steuerung)

Im zentralen Betriebsmodell verbleibt die datenschutzrechtliche Verantwortlichkeit bei den fachlich entscheidenden Landesbehörden, die Zwecke und wesentliche Mittel der Verarbeitung bestimmen. Die FITKO erbringt demgegenüber Transport- und Plattformleistungen als Auftragsverarbeiterin und trifft keine inhaltlichen Fachentscheidungen. Der zentrale Betreiber wird als Unterauftragsverarbeiter in die Leistungserbringung eingebunden.

Dieses Rollenbild wird durch die Zielarchitektur technisch gestützt: Eine strikte Trennung von Fach- und Betriebsdaten sowie eine Ende-zu-Ende-Verschlüsselung stellen sicher, dass die Entscheidungshoheit der Länder gewahrt bleibt und die FITKO ausschließlich im Rahmen weisungsgebundener Verarbeitung tätig wird.

Aus der Auftragsverarbeiterrolle folgen für die FITKO klare Steuerungs-, Kontroll- und Dokumentationspflichten (Art. 28 DSGVO). Sie hat Weisungen der Verantwortlichen umzusetzen, den Unterauftragsverarbeiter sorgfältig auszuwählen und fortlaufend zu überwachen, geeignete technische und organisatorische Maßnahmen vorzugeben und deren Wirksamkeit regelmäßig

zu prüfen. Gegenüber den verantwortlichen Behörden bleibt die FITKO für die Einhaltung der Pflichten durch den Unterauftragsverarbeiter voll verantwortlich.

Der zentrale Betrieb setzt ferner definierte Netz- und Betriebsanforderungen voraus. Transportinfrastruktur und Backend sind an das Verbindungsnetz anzuschließen; Sicherheitsanforderungen (einschließlich Protokollierung, Angriffserkennung, Härtung, Patch- und Vulnerability-Management) sind verbindlich festzulegen und nachprüfbar zu machen. Näheres ist in den Abschnitten II.1 und III.1. dargestellt, auf die hier verwiesen wird.

3.2. Haftungslage

3.2.1. Außenhaftung gegenüber Betroffenen (Art. 82 DSGVO)

Für das Außenverhältnis gegenüber betroffenen Personen gilt die gesamtschuldnerische Haftung nach Art. 82 Abs. 4 DSGVO. Betroffene können den vollen Schaden von jedem an der Verarbeitung Beteiligten verlangen. Auftragsverarbeiter haften allerdings nur, soweit sie eigene Pflichten verletzen oder rechtmäßige Weisungen missachten; eine Exkulpation ist möglich, wenn sie in keinerlei Hinsicht für den Schaden verantwortlich sind (Art. 82 Abs. 3 DSGVO).

Haftungsbeschränkungen gegenüber Betroffenen sind unzulässig und berühren den gesetzlichen Anspruch nicht.

3.2.2. Innenverhältnis und Regress

Im Innenverhältnis zwischen verantwortlichen Behörden, FITKO und zentralem Betreiber ist eine vertragliche Regressordnung vorzusehen, die die Verteilung von Kosten und Schäden kausalitäts- und verschuldensorientiert regelt (Art. 82 Abs. 5 DSGVO).

Dazu gehören klare Vorgaben für Incident-Governance (Meldeketten, Forensik, Abhilfe- und Benachrichtigungspflichten), Nachweise und Mitwirkung, ein transparenter Kostenkatalog (u.a. technische Analysen, Rechtsberatung, Benachrichtigung, Kommunikationsmaßnahmen) sowie Mechanismen zur Streitbeilegung. Die Einbindung eines Unterauftragsverarbeiters ändert an der Einstandspflicht der FITKO gegenüber den Verantwortlichen nichts. Im Innenverhältnis können Rückgriffe auf den Unterauftragsverarbeiter nach dessen Verantwortungsbeitrag vereinbart werden.

Soweit die FITKO als öffentliche Stelle im Rahmen der Erfüllung öffentlicher Aufgaben tätig wird, sind behördliche Geldbußen nach nationalem Recht regelmäßig ausgeschlossen. Dies lässt die

zivilrechtliche Haftung nach Art. 82 DSGVO unberührt; insbesondere bleibt der Schadensersatzanspruch der betroffenen Personen bestehen.

3.3. Vertragsgestaltung

Die rechtliche Einordnung erfordert eine konsistente Vertragskaskade von der Behörde zum Unterauftragsverarbeiter.

3.3.1. AVV (FITKO -> Behörde)

Zwischen den verantwortlichen Behörden und der FITKO ist ein Auftragsverarbeitungsvertrag (AVV) mit detaillierten Weisungs-, Informations-, Audit-, Sub-Processor-, Sicherheits-, Exit- und Reversibilitätsregelungen zu schließen. Sicherheitsanhänge müssen verbindlich die Verfügbarkeitsziele, Monitoring-, Logging- und Patch-Prozesse sowie das Schlüssel- und Kryptokonzept festlegen.

3.3.2. Unterauftragsvereinbarung (Betreiber -> FITKO)

Die Unterauftragsvergabe an den zentralen Betreiber ist in einer Unterauftragsvereinbarung abzubilden, die Durchgriffspflichten der FITKO, Prüf- und Nachweisrechte, Anforderungen an Netz- und Rechenzentrumsbetrieb, Zertifizierungs- und Compliance-Nachweise sowie besondere Pflichten zur Datenlokation und Reversibilität enthält.

3.3.3. Regress- und Freistellungsregelung

Ergänzend ist eine Regress- und Freistellungsregelung zu vereinbaren, die die Verteilung im Innenverhältnis nach Verursachung und Verschulden ausgestaltet, ohne den gesetzlichen Außenanspruch von Betroffenen zu beschneiden.

3.4. Verweise

Die vorstehenden Ausführungen konsolidieren Ergebnisse aus anderen Teilen des Gutachtens. Zum Rollenbild und zur datenschutzrechtlichen Verantwortlichkeit wird auf den Abschnitt II.1 verwiesen. Die dogmatischen Grundlagen der Haftung und die Ausgestaltung des Innenregresses sind im Abschnitt II.8 vertieft dargestellt. Anforderungen an Netze, Betrieb und Zertifizierungen (einschließlich Verbindungsnetz-Anschluss und Sicherheitsnachweise) ergeben sich aus den Abschnitten III.1 und 2.

***

D. Zusammenfassende Gesamtschau der rechtlichen Bewertung

Nachfolgend fassen wir den wesentlichen rechtlichen Rahmen (I.) und die wesentlichen Ergebnisse des Gutachtens (II.) zur Orientierung zusammen. Für die Einzelheiten wird auf das Gutachten verwiesen.

I. Rechtlicher Rahmen

Für die Neukonzeption und den Betrieb von OSiP ist ein komplexes Geflecht aus europäischen und nationalen Normen zu beachten. Der rechtliche Rahmen gliedert sich im Wesentlichen in fünf Bereiche:

1. Verfassungsrechtliche und organisatorische Grundlagen

Die Zusammenarbeit von Bund und Ländern bei OSiP fußt auf der föderalen Kompetenzordnung des Grundgesetzes.

- **Art. 91c GG (Informationstechnik):** Diese Verfassungsnorm bildet die Basis für die IT-Zusammenarbeit von Bund und Ländern. Sie erlaubt das Zusammenwirken bei Betrieb und Entwicklung von IT-Systemen (Abs. 1) und den gemeinschaftlichen Betrieb (Abs. 3) sowie die Festlegung von Standards (Abs. 2).
- **IT-Staatsvertrag (IT-StV):** Er konkretisiert Art. 91c GG und etabliert den IT-Planungsrat als Steuerungsgremium sowie die FITKO als operative Unterstruktur. Beschlüsse des IT-Planungsrats zu Standards und Sicherheitsanforderungen sind hierdurch rechtlich verbindlich.
- **Verbot der Mischverwaltung:** Die fachlichen Entscheidungen müssen bei den zuständigen Landesbehörden verbleiben; die FITKO darf lediglich technische Unterstützungsleistungen erbringen.

2. Datenschutzrecht

Die anzuwendenden datenschutzrechtlichen Grundsätze sind im Ergebnis für alle Anwendungsfälle und Beteiligten im Wesentlichen gleich aufgrund der Vereinheitlichung durch die DSGVO und der Harmonisierung durch die JI-Richtlinie (wobei im Bereich der nationalen Sicherheit das EU-Datenschutzrecht gar nicht unmittelbar gilt). Das konkret anwendbare Datenschutzregime ist jedoch abhängig vom jeweiligen Anwendungsfall (z. B. gewerbliche Zuverlässigkeit vs. nach-

richtendienstliche Tätigkeit) und vom jeweils betrachteten Beteiligten (für die eine ZSÜ durchführende Behörde und die mitwirkenden Behörden bzw. Erkenntnisstellen gilt jeweils das auf diese Stelle anwendbare Bundes- oder Landesrecht).

- **DSGVO (EU):** Gilt grundsätzlich für die meisten Anwendungsfälle (z. B. Luftsicherheit, Hafen, Gewerbe) unmittelbar. Ausgenommen vom Anwendungsbereich der DSGVO sind die nationale Sicherheit (zu der Sicherheitsüberprüfungen regelmäßig gehören) und die Strafverfolgung (die einzelne weitere Anwendungsfälle betrifft); zum Teil gibt es allerdings Verweise aus dem deutschen Recht, die die DSGVO auch insoweit zur Anwendung bringen.
- **JI-Richtlinie (Justiz/Inneres):** Für Bereiche der Strafverfolgung und des Strafvollzugs (z. B. Justizvollzugsanstalten) gilt nicht die DSGVO, sondern die nationalen Umsetzungen der JI-Richtlinie (Teil 3 BDSG bzw. die entsprechenden landesrechtlichen Vorschriften in den LDSG, Polizeigesetze etc.).
- **Sicherheitsüberprüfungsgesetze (SÜG):** Sicherheitsüberprüfungen, insbesondere nach SÜG, dienen regelmäßig der nationalen Sicherheit und sind außerhalb des Anwendungsbereichs der DSGVO. Hier gelten spezialgesetzliche Datenschutzregeln des SÜG und selektiv das BDSG.
- **BDSG und LDSG:** Ergänzen – soweit anwendbar – die DSGVO und regeln die Datenverarbeitung der öffentlichen Stellen von Bund und Ländern.

3. IT-Sicherheitsrecht

Die Sicherheitsanforderungen sind aufgrund der Sensibilität der Daten (Art. 10 DSGVO) und der Bedeutung für die staatliche Sicherheit sehr hoch. Überschlägig sind folgende Rechtsquellen zu nennen:

- **IT-Netzgesetz (IT-NetzG):** Schreibt für den Datenaustausch zwischen Bund und Ländern zwingend die Nutzung des Verbindungsnetzes vor. OSiP muss daher direkt an das Verbindungsnetz angeschlossen werden.
- **BSI-Gesetz (BSIG) & KRITIS (NIS-2):** Der OSiP-Betreiber wird künftig voraussichtlich als „wichtige" oder „besonders wichtige Einrichtung" unter die NIS-2-Regulierung fallen. Für Bundesbehörden gelten zudem die Mindeststandards des BSI verbindlich.
- **Beschlüsse des IT-Planungsrats:**

  - **Leitlinie Informationssicherheit:** Verpflichtet zur Anwendung des IT-Grundschutzes (BSI).
  - **Föderale IT-Architekturrichtlinie:** Setzt verbindliche Vorgaben für Architektur, Sicherheit und digitale Souveränität.
- **OZG, ITSiV-PV und OZSV:** Für einen etwaigen Online-Antragsdienst (Frontend für Bürger bzw. Unternehmen) gelten das Onlinezugangsgesetz (OZG) und darüber die IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) und die Verordnung über Standards für den Onlinezugang zu Verwaltungsdiensten (OZSV), die ihrerseits auf einschlägige Normen u.a. des BSI verweist.

4. Geheimschutz (Verschlusssachen)

Da über OSiP auch Erkenntnisse ausgetauscht werden, die als VS-NfD eingestuft sind, gelten besondere Schutzvorschriften.

- **SÜG (Bund/Länder):** Regeln die materiellen Voraussetzungen für den Geheimschutz.
- **Verschlusssachenanweisung (VSA):** Verwaltungsvorschriften, die technische Maßnahmen für die Übermittlung von VS vorschreiben (z. B. BSI-zugelassene Kryptografie, Freigabe von IT-Systemen).

5. Fachrechtliche Rechtsgrundlagen (Auswahl)

Die eigentliche Rechtsgrundlage für die Datenverarbeitung findet sich in den Fachgesetzen, die die Überprüfung anordnen. Diese bestimmen Zweck, Umfang und zuständige Stellen. Wichtige Beispiele sind:

- Luftsicherheitsgesetz (LuftSiG) und Atomgesetz (AtG).
- Waffengesetz (WaffG) und Sprengstoffgesetz (SprengG).
- Hafensicherheitsgesetze der Länder.
- Sicherheitsüberprüfungsgesetze (SÜG) des Bundes und der Länder (für geheimschutzbetreute Tätigkeiten).
- Gewerbeordnung (GewO) und Prostituiertenschutzgesetz (ProstSchG).

II. Wesentliche Ergebnisse

Die nachfolgende Zusammenfassung bündelt wesentliche Ergebnisse der rechtlichen Prüfung (Teil C). Sie beantwortet zentrale Fragestellungen der FITKO zur Machbarkeit der Zielarchitektur, zur Verteilung der Verantwortlichkeiten sowie zu den zwingenden Anforderungen an Technik, Betrieb und Sicherheit. Für Details wird auf das Gutachten unter C. verwiesen.

1. Verfassungsrechtliche Zulässigkeit des zentralen Betriebs

Die geplante Neukonzeption von OSiP als zentraler Dienst unter Steuerung der FITKO ist verfassungsrechtlich zulässig.

- **Rechtsgrundlage:** Der zentrale Betrieb stützt sich auf Art. 91c GG (Zusammenarbeit bei IT-Systemen) in Verbindung mit dem IT-Staatsvertrag und den verbindlichen Beschlüssen des IT-Planungsrats.
- **Wahrung der Kompetenzordnung:** Das Verbot der Mischverwaltung wird gewahrt, da die FITKO (bzw. der technische Betreiber) ausschließlich technische Unterstützungsleistungen erbringt. Die fachlichen Sachentscheidungen (Durchführung und Ergebnis der Zuverlässigkeits- und Sicherheitsüberprüfung – ZSÜ) verbleiben vollständig bei den zuständigen Landes- und Bundesbehörden.
- **Technische Parametrisierung:** Da das Fachrecht der Länder (insb. die Sicherheitsüberprüfungsgesetze) unterschiedliche Vorgaben zu Fristen, Löschung, Aktenführung und organisatorischer Trennung macht, ist ein zentraler Betrieb nur zulässig, wenn die Software mandantenfähig ist und länderspezifische Konfigurationen (Policies) technisch erzwingen kann.

2. Datenschutzrechtliches Verantwortungsmodell

Da für die FITKO keine gesetzliche Grundlage existiert, um Inhaltsdaten von Sicherheitsüberprüfungen eigenverantwortlich zu verarbeiten, ist das Modell der Auftragsverarbeitung zu wählen.

- **Rollenverteilung:** Die nutzenden Behörden (Genehmigungs- und Erkenntnisstellen) sind datenschutzrechtlich jeweils getrennt Verantwortliche (Art. 4 Nr. 7 DSGVO). Die FITKO agiert als Auftragsverarbeiterin (Art. 28 DSGVO) für die Bereitstellung der Plattform. Der technische Dienstleister (Rechenzentrum/Cloud-Provider) kann als Unterauftragsverarbeiter der FITKO eingebunden werden.

- **Vertragskette:** Empfohlen wird ein Kettenmodell. Dabei sind Auftragsverarbeitungsverträge (AVV) zwischen den nutzenden Stellen und der FITKO erforderlich. Die FITKO muss die Datenschutzpflichten vertraglich an den technischen Betreiber weiterreichen („Back-to-Back") und sich Kontrollrechte sichern.
- **Ende-zu-Ende-Verschlüsselung (E2EE):** Sofern eine durchgängige E2EE implementiert ist und die FITKO keinen Zugriff auf Schlüssel hat, ist mit guten Gründen davon auszugehen, dass sie keine personenbezogenen Daten im Sinne des Datenschutzrechts, sondern nur anonyme Daten verarbeitet (relative Anonymität). Dennoch wird aus Gründen der Rechtssicherheit empfohlen, auch in diesem Fall eine Auftragsverarbeitung zu vereinbaren (u.a. mit Blick auf: personenbezogene Metadaten oder Nutzerdaten; potentielle zukünftige Entschlüsselungsmöglichkeiten; technisch-organisatorische Schutzpflichten zur Gewährleistung der Anonymität).

3. Datenschutz-Folgenabschätzung (DSFA)

Aufgrund der sensiblen Daten (u.a. Art. 10 DSGVO: strafrechtliche Verurteilungen/Straftaten) und der Eingriffstiefe besteht ein hohes Risiko, weshalb eine DSFA zwingend durchzuführen ist.

- **Zuständigkeit:** Verpflichtet sind die nutzenden Fachbehörden als Verantwortliche.
- **Vorgehensmodell:** Es wird empfohlen, dass die FITKO eine zentrale Muster-DSFA (bzw. Baustein-DSFA) für die Plattform erstellt, welche die technischen Risiken und Maßnahmen dokumentiert. Die Länder übernehmen dieses Muster und ergänzen es um ihre spezifischen Prozesse.

4. IT-Sicherheit, Netzinfrastruktur und Verschlüsselung

Für OSiP gelten aufgrund der Einstufung von Teilen der Daten als Verschlusssache (VS-NfD) und des allgemein hohen Schutzbedarfs sehr strenge Sicherheitsanforderungen. Hierzu zählen:

- **Verbindungsnetz:** Der Datenaustausch zwischen Bund und Ländern muss gemäß § 3 Abs. 1 IT-NetzG zwingend über das Verbindungsnetz (bzw. angeschlossene sichere Verwaltungsnetze) erfolgen. Ein Betrieb des Backends/Transportdienstes mit direkter Anbindung an das offene Internet ist unzulässig. Eine Ausnahme gilt nur für den OZG-Antragsdienst (Frontend für Bürger).
- **Verschlüsselung:** Es ist eine Ende-zu-Ende-Verschlüsselung (E2EE) der Inhaltsdaten anzustreben.

- **Adapter:** Wo E2EE technisch nicht möglich ist (z. B. bei Adaptern zur Format-Konvertierung), muss die Verschlüsselungsunterbrechung kompensiert werden. Empfohlen wird der Betrieb solcher Adapter im Hoheitsbereich der sendenden Stelle oder eine Gateway-to-Gateway-Verschlüsselung, um den Zugriff Dritter auszuschließen.
- **Standards:** Die Einhaltung der BSI-Standards (IT-Grundschutz) und der Leitlinie Informationssicherheit des IT-Planungsrats ist für das gesamte Verfahren verbindlich.

5. Anforderungen an Betreiber und Cloud-Nutzung

Ein Betrieb durch private Dienstleister oder in einer Cloud-Umgebung ist rechtlich nicht ausgeschlossen, unterliegt aber strengen Auflagen zur Gewährleistung der Digitalen Souveränität und Sicherheit.

- **Zertifizierung:** Der Betreiber muss seine Eignung durch Zertifikate nachweisen. Erforderlich sind ISO 27001 auf Basis von IT-Grundschutz (insb. Profil „VN-TNA“ für den Netzanschluss) und bei Cloud-Komponenten ein aktuelles C5-Testat.
- **KRITIS / NIS-2:** Der Betreiber wird voraussichtlich als „wichtige“ oder „besonders wichtige Einrichtung“ unter die kommende NIS-2-Regulierung (BSIG-E) fallen und muss entsprechende Risikomanagement-, Melde- und Lieferkettenprozesse nachweisen.
- **Datenlokation:** Ein Betriebsstandort in Deutschland ist im Hinblick auf die Netzstrategie 2030 (Nationales Routing) und die Sensibilität der Daten dringend zu empfehlen. Drittlandtransfers sollten vermieden werden.
- **Exit-Strategie:** Vertragliche Regelungen müssen sicherstellen, dass ein Anbieterwechsel ohne Datenverlust möglich ist (Vermeidung von Vendor-Lock-In).

6. Sonstiges: Zustimmungserklärung und Haftung

- **Zustimmung:** Die in vielen Anwendungsfällen geforderte Zustimmung der betroffenen Person ist eine fachliche Verfahrensvoraussetzung (aber keine Einwilligung im Sinne der DSGVO). Da Formvorschriften variieren (einige Länder verlangen Schriftform, andere erlauben elektronische Form), muss OSiP hybride Prozesse unterstützen (Upload von Scans vs. eIDAS-konforme elektronische Signatur).
- **Haftung:** Im Außenverhältnis haften Verantwortliche und Auftragsverarbeiter gesamtschuldnerisch (Art. 82 DSGVO). Im Innenverhältnis sollte eine vertragliche Regressordnung

vereinbart werden, die sich an Verursachung und Verschulden orientiert. Die Gestaltungsmöglichkeiten sind aber beschränkt.

Fazit: Die geplante Zielarchitektur ist rechtlich tragfähig. Empfohlen wird die Umsetzung als zentraler Dienst der FITKO im Modell der Auftragsverarbeitung, technisch abgesichert durch Ende-zu-Ende-Verschlüsselung, Anbindung an das Verbindungsnetz und ein BSI-konformes Sicherheitskonzept, das die Mandantentrennung für die Länder garantiert.

E. Glossar / Abkürzungsverzeichnis

AES	Antrags- und Erfassungsstruktur (OSiP-Datenformat)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AtG	Atomgesetz
AVn	Allgemeine Vorgaben (gemäß Nationaler/Föderaler IT-Architektur-richtlinie)
AVV	Auftragsverarbeitungsvereinbarung
AZR	Ausländerzentralregister
beA	Besonderes elektronisches Anwaltspostfach
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben AöR
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BO-Client	Back Office Client
BRAK	Bundesrechtsanwaltskammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BSIG-E	Entwurf des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BZR	Bundeszentralregister
CRA	Cyber Resilience Act (VO (EU) 2024/2847)

CSG	Cybersicherheitsgesetz für die Cybersicherheit in Baden-Württemberg
DSFA	Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
DSGVO	Datenschutz-Grundverordnung (VO (EU) 2016/679)
DSK	Datenschutzkonferenz
DVC	Deutsche Verwaltungscloud, föderales Rahmenkonzept und Governance-Modell für Cloud-Dienste der öffentlichen Verwaltung
E2EE	End-to-End Encryption (Ende-zu-Ende-Verschlüsselung)
EDPB	European Data Protection Board (Europäischer Datenschutzausschuss)
EKS	Erkenntnisstruktur
EKS-Client	OSiP-Client für Erkenntnisstellen
EuGH	Europäischer Gerichtshof
FB	Fachbehördenstruktur
FIT-AB	Föderales IT-Architekturboard
FITKO	Föderale IT-Kooperation AöR
FITKO-AM	Föderales IT-Architekturmanagement der FITKO
FO-Client	Front Office Client (von OSiP, für Antragserfassung)
G2EE	Gateway-To-End-Encryption
G2GE	Gateway-To-Gateway-Encryption
GG	Grundgesetz für die Bundesrepublik Deutschland
GZR	Gewerbezentralregister
IAM	Identity and Access Management (Identitäts- und Zugriffsmanagement)
ISB	Informationssicherheitsbeauftragte(r)
ISMS	Informationssicherheitsmanagementsystem
ISR ITKB	Informationssicherheitsrichtlinie IT-Konsolidierung Bund

IT-PLR	IT-Planungsrat
IT-StV	IT-Staatsvertrag (Vertrag zur Ausführung von Art. 91c GG)
IVÖV	Informationsverbund der öffentlichen Verwaltung
JVollzDSG NRW	Justizvollzugs-Datenschutzgesetz NRW
KoSIT	Koordinierungsstelle für IT-Standards
KRITIS	Kritische Infrastruktur(en)
LDSG	Landesdatenschutzgesetz(e)
LfV	Landesamt/Landesämter für Verfassungsschutz
LKÄ	Landeskriminalämter
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz)
MLS	Messaging Layer Security
NEOSiP	Zukünftige Version von OSiP
NIS-RL	EU-Cybersicherheitsrichtlinie (Network and Information Security Directive), RL (EU) 2016/1148 – aufgehoben durch die NIS2-RL
NIS2-RL	EU-Cybersicherheitsrichtlinie (Network and Information Security Directive), RL (EU) 2022/2555
NIS2UmsuCG	NIS2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz
OLG	Oberlandesgericht
OSCI	Online Services Computer Interface
OSiP	Online-Sicherheitsprüfung
OZG	Online-Zugangsgesetz
PaaS	Platform as a Service
RAVPV	Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer

REST	Representational State Transfer (Software-Architekturparadigma, relevant für Maschine-zu-Maschine-Kommunikation)
SaaS	Software as a Service
SDM	Standard-Datenschutz-Modell
SOAP	Netzwerkprotokoll für Datenaustausch (früher: Simple Object Access Protocol)
SÜG	Sicherheitsüberprüfungsgesetz
TLS	Transport Layer Security
TOM	Technische und Organisatorische Maßnahmen (Art. 32 DSGVO)
VSA	Verschlusssachenanweisung (Allgemeine Verwaltungsvorschrift zum Geheimschutz)
VS-NfD	Verschlusssache – NUR FÜR DEN DIENSTGEBRAUCH
XPS3	Proxy-Plattform für den Datenaustausch zwischen den Landes-OSiP-Kernen und den zentralen Erkenntnisstellen (zentrale Datendrehscheibe)
XRepository	Zentrale Standardisierungs- und Referenzplattform für XÖV-Spezifikationen und weitere IT-Standards der öffentlichen Verwaltung
XTA	XML Transport Adapter
XÖV	XML in der öffentlichen Verwaltung
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister
ZSÜ	Zuverlässigkeits- und Sicherheitsüberprüfung

Anlage 1

Relevante Rechtsgrundlagen und Implikationen für OSiP

I. Datenschutz (EU/Bund/Land)

Gesetz/ Regelungs-bereich	Gesetzgeber	Vollzug/Ausführung	Verwaltungsform	Besondere Hinweise (Implikationen für Architek-tur/Betrieb)
DSGVO (VO (EU) 2016/679)	EU	Anwendung durch Bundes- und Landesbehörden Aufsicht: BfDI; Datenschutz-Auf-sichtsbehörden der Länder	Unmittelbar geltendes Unionsrecht; verbind-lich für Bundes- und Landesverwaltung	OSiP muss so gestaltet sein, dass die nutzenden Stellen die Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO) einhalten und dies nachweisen können (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Art. 25 (Privacy by Design/Default) und Art. 32 (TOM) verlangen eine ISMS-gestützte Architektur (Rollen-/Rechtemodell, Protokollierung, Lösch-/Sperrkonzepte; systemseitige Abbildung von Da-tenminimierung und Zweckbindung). Diese Anfor-derungen sind in OSiP technisch-organisatorisch umzusetzen (inkl. nachvollziehbarer Protokolle und Policy-Durchsetzung). Grundsätzlich muss der Dienstleister als Auf-tragsverarbeiter sorgfältig ausgewählt und ver-pflichtet werden (Art. 28 DSGVO).
BDSG	Bund	Anwendung durch Bundesbehör-den Aufsicht: BfDI	Bundesverwaltung	Das BDSG ergänzt und konkretisiert die DSGVO auf Basis von Öffnungsklauseln. Für OSiP ist eine logische und technische Mandantentrennung zwi-

				schen Bundes- und Landesmandanten als Architektur-Soll vorzusehen (Ableitung aus DSGVO-Grundsätzen, nicht Gesetzeswortlaut).
Landesdatenschutzgesetze (LDSG/DSG der Länder)	Länder	Landesbehörden Landesaufsichten	Ländereigene Verwaltung	Die Landesdatenschutzgesetze ergänzen und konkretisieren die DSGVO für den Landesvollzug und enthalten teils weitergehende Pflichten (z.B. zu Protokollierung/Informationspflichten). OSiP sollte landesspezifische Policies parametrisierbar abbilden.
JI-Richtlinie (EU) 2016/680 – nationale Umsetzungen (z.B. JVollzDSG NRW)	EU/Bund/Land	Justiz/Strafverfolgung/Strafvollzug	Richtlinie mit nationaler Umsetzung	Für Verfahren im Anwendungsbereich der JI-Richtlinie gelten die jeweiligen nationalen/landesrechtlichen Umsetzungsgesetze; die DSGVO gilt dort nicht unmittelbar. Für OSiP sind getrennte Datenräume/Prozesse, differenzierte Rechtsgrundlagen-Profile und abgestufte Logging-Profile vorzusehen.
SÜG (Bund) – Datenschutzspezialrecht	Bund	Bundesstellen; Mitwirkung BfV/MAD/BND	Bundesverwaltung	Spezielle Datenschutz-/Protokollierungspflichten (insb. § 36 SÜG) und strikte Geheimschutzvorgaben. Für OSiP bedeutet das: VS-NfD-taugliche Ende-zu-Ende-Strecken, Geheimschutz-Rollen-/Berechtigungskonzepte, besonders strenge Protokollierung. Maßgeblich ist außerdem die Verschlusssachenanweisung (VSA)..

II. **Datenschutzrecht für die OSiP-Anwendungsfälle**

Anwendungsfall	Zweck	Anwendbarkeit der DSGVO	Anwendbarkeit BDSG/LDSG	Datenschutzregelungen im Fachrecht

Sicherheitsüberprüfung (SÜG Bund)	nationale Sicherheit	**Nein** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (-) [§ 36 Abs. 1 Nr. 1 SÜG]	**BDSG** (jedoch nur, soweit gem. § 36 SÜG anwendbar)	
MADG	nationale Sicherheit	**Nein** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (-) [§ 36 Abs. 1 Nr. 1 SÜG]	**BDSG** (jedoch nur, soweit gem. § 36 SÜG anwendbar)	
Atomrecht (§ 12b AtG)	u.a. nationale Sicherheit (§ 1 Nr. 3 AtG)	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO; es sei denn, man verortet § 12b AtG im Anwendungsbereich des Euratom-Vertrags] entsprechend (+) [über LDSG]	**LDSG** (BDSG für beteiligte Bundes-behörden)	**Ja** (§ 12b Abs. 6 AtG: Prinzip der Erforderlichkeit; Abs. 9: Verordnungsermächtigung)
Luftsicherheit	nationale Sicherheit (vgl. § 1 LuftSiG)	**Ja** unmittelbar (+) [wohl im Anwendungsbereich des Unionsrechts, s. Art. 100 Abs. 2 AEUV und Art. 2 Nr. 15 VO (EG) 300/2008 (und Anhang 4 Ziff. 1.2. Nr. 4] jedenfalls entsprechend	**LDSG** (BDSG für beteiligte Bundesbehörden)	

		(+) [über LDSG]		
Hafensicherheit (z.B. §§ 16 ff. BremHaSiG; §§ 17 ff. HaSiG NRW; §§ 14 ff. HmbHafenSG; §§ 11 ff. NHafenSG)	nationale Sicherheit (vgl. § 1 Satz 1 BremHaSiG; § 1 HaSiG NRW; § 1 Abs. 1 HmbHafenSG)	**Ja** unmittelbar (+) [wohl im Anwendungsbereich des Unionsrechts, s. Art. 100 Abs. 2 AEUV und Art. 16 Abs. 2 RL 2005/65/EG] jedenfalls entsprechend (+) [über LDSG]	**LDSG** (mit Spezialvorschriften in den Hafensicherheitsgesetzen)	
Sprengstoffgesetz (§ 8a SprengG)	u.a. nationale Sicherheit	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]	**BDSG** (für Bundesbehörden) **LDSG** (für Landesbehörden)	
Bewachungsgewerbe (§ 34a GewO)	öffentliche Sicherheit, wohl auch nationale Sicherheit	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]	**LDSG**	
Waffenrecht (§ 5 WaffG)	öffentliche Sicherheit (§ 1 Abs. 1 WaffG), aber auch nationale Sicherheit	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]	**LDSG**	
Jagd (§ 17 Abs. 1 Satz 2	öffentliche Sicherheit (§ 1 Abs. 1 WaffG), aber auch nationale	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit.	**LDSG**	

JagdG, § 5 WaffG)	Sicherheit	a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]		
Aufenthalt (§§ 73 Abs. 2, 3 AufenthG)	öffentliche Sicherheit, wohl auch nationale Sicherheit	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]	**LDSG**	
Einbürgerung (§ 37 StaG)	öffentliche Sicherheit, wohl auch nationale Sicherheit	**Ja (entsprechend)** unmittelbar (-) [Art. 2 II lit. a DSGVO] entsprechend (+) [über § 1 Abs. 8 BDSG]	**LDSG**	
Justizvollzug (§§ 21 f. JVollzDSG NRW)	Aufrechterhaltung der Sicherheit	**Nein** unmittelbar (-) [Art. 2 II lit. d DSGVO] entsprechend (-) [NRW: s. JVollzDSG]	(NRW: LDSG nur durch punktuelle Verweise)	
Anlassbezogene Überprüfungen (NRW: Akkreditierungsverfahren mit Zuverlässigkeitsüberprüfungen auf Basis einer Einwilligung)	öffentliche Sicherheit	**Nein** unmittelbar (-) [Art. 2 II lit. d DSGVO]	(NRW: LDSG)	
Prostitutionsgewerbe	öffentliche Sicherheit	**Ja**	**LDSG**	

(§ 15 ProstSchG)		unmittelbar (+)		

III. Fachrecht (OSiP-Anwendungsfälle)

Gesetz/ Regelungsbereich	Gesetzgeber	Vollzug/Ausführung	Verwaltungsform	Besondere Hinweise (Implikationen für Architektur/Betrieb)
Sicherheitsüberprüfungsgesetz (SÜG, Bund)	Bund	Bundesstellen; Mitwirkung BfV/MAD/BND	Bundesverwaltung	Erfordert Geheimschutz/VS-IT-Vorgaben, restriktive Datenweitergaben und revisionssichere Protokollierung. OSiP muss VS-NfD-geeignete Transportwege, definierte Geheimschutz-Workflows und strenge Berechtigungskonzepte bereitstellen.
Landessicherheitsüberprüfungsgesetze (LSÜG/SÜG der Länder)	Länder	Zuständige Landesstellen; Mitwirkung LfV	Ländereigene Verwaltung	Im Kern analog zum Bund, mit länderspezifischen Zuständigkeiten/Verfahrensschritten. OSiP sollte länderweise konfigurierbare Profile (Abläufe, Schriftgutverwaltung, Fristen/Prüfschritte) vorsehen.
MADG (militärischer Bereich)	Bund	MAD/BMVg	Bundesverwaltung	Klare Bereichstrennung zivil/militärisch im Systemdesign; Schnittstellen zum SÜG beachten.
Luftsicherheitsgesetz (LuftSiG) (z.B. § 7, § 16)	Bund	Länder als Luftsicherheitsbehörden; LBA in Teilbereichen	Ländereigene Verwaltung, punktuell Bund	Landesspezifische Rechtsgrundlagen → je Land getrennte Mandanten/Rechtsgrundlagen in OSiP.
Hafensicherheitsgesetze (z.B. HaSiG NRW, HmbHafenSG,	Länder	Zentrale Hafensicherheitsbehörden; Polizei/WSP	Ländereigene Verwaltung	RL 2005/65/EG; länderspezifisches Datenschutz-Fachrecht → getrennte Rechtsgrundlagen je Land im Mandantenmodell.

BremHaSiG, NHafenSG)				
Atomgesetz (§ 12b AtG)	Bund	Länder im Auftrag des Bundes; teils Bund	Auftragsverwaltung	Durchgängig gelten: nachvollziehbare Rechtsgrundlagen je Verarbeitungsschritt, beweisfeste Protokollierung, Fristen-/Wiederholungsprüfungen, Beteiligungs-APIs und strikte Zweckbindung/Mandantierung. (Ausprägungen variieren je Landesvollzug.)
Sprengstoffgesetz (SprengG)	Bund	Überwiegend Länder (ZustVO)	Ländereigene Verwaltung	Erlaubnisse/Überwachung: beweissichere Protokolle, Fristen-/Wiederholungsprüfung, Nachberichtsmechanismen.
Waffenrecht (WaffG)	Bund	Länder (Waffenbehörden); BKA-Feststellungen	Ländereigene + Bundesverwaltung	Integration BKA-Feststellungen; strikte Trennung „Erkenntnisstelle"/„Entscheidung".
Bewachungsgewerbe (§ 34a GewO/BewachV)	Bund	Länder (örtliche Ordnungs-/Gewerbebehörden)	Ländereigene Verwaltung	Erlaubniserteilung, Zuverlässigkeitsprüfung, Echtzeitprüfungen gegen Register → standardisierte EKS-Schnittstellen.
Bundesjagdgesetz / Jagdrecht	Bund/Länder	Untere Jagdbehörden	Ländereigene Verwaltung	Landesausgestaltung beachten; Wiederverwendung Prüfbausteine (Zuverlässigkeit/Waffen).
Staatsangehörigkeitsgesetz (StAG) (z.B. § 37)	Bund	Länder (Staatsangehörigkeitsbehörden); BVA in Auslandsfällen	Ländereigene + Bundesverwaltung	Beteiligungsverfahren mit Sicherheitsbehörden → transparente Beteiligungs-APIs, Friststeuerung.
Aufenthaltsgesetz (allg.; § 73, § 73b)	Bund	Ausländerbehörden (Länder); AA (Visum)	Ländereigene + Bundesverwaltung	Orchestrierung mehrerer Stellen; strenge Protokollierung/Beauskunftung.
Prostituiertenschutzgesetz (ProstSchG)	Bund	Länder/Kommunen (Ordnungs-/Gesundheitsbehörden)	Ländereigene Verwaltung	Getrennte Datenarten (Gesundheitsberatung vs. Erlaubnis) → strikte Zwecke/Mandantierung.

Justizvollzug (z.B. JVollzDSG NRW)	Land	Justizvollzugsanstalten	Ländereigene Verwal-tung	JI-Regime, nicht DSGVO-unmittelbar → gesonderte Datenschutz-Profile/Protokolle.

Anlage 2

I. IT-Sicherheitsrecht (EU)

Gesetz/ Regelungs-bereich	Normgeber	Vollzug/Ausführung	Verwaltungsform	Besondere Hinweise (Implikationen für Architek-tur/Betrieb)
Cybersecurity Act (VO (EU) 2019/881)	EU	ENISA; EU-Zertifizierungsrahmen	Verordnung	EU-Zertifizierungsschemata sind bei Beschaf-fung/Betrieb zu berücksichtigen. EUCC (Common-Criteria-basiertes EU-Schema) wurde durch Durch-führungs-VO (EU) 2024/482 eingeführt; konsoli-dierte Fassung seit 08.01.2025. Relevanz für Kom-ponenten/Dienste von OSiP prüfen.
NIS2-Richtlinie (RL (EU) 2022/2555) + Durchführungs-VO (Art. 21 Abs. 5)	EU	Nationale Umsetzung (NIS2UmsG; BSIG n. F.)	Richtlinie	Für (besonders) wichtige Einrichtungen u.a. Pflich-ten zu Risiko-, Asset-, Patch-, Logging- und Inci-dent-Management sowie Berichtspflichten. Für O-SiP sind ISMS-Integration, PSIRT-/SoC-Prozesse und Nachweisführung vorzusehen. (Stand DE-Um-setzung: Regierungsentwurf.)
CER-Richtlinie (RL (EU) 2022/2557)	EU	Nationales KRITIS-DachG	Richtlinie	Ergänzt NIS-2 um physische Resilienz; in OSiP mit NIS-2-Risikomanagement zu verzahnen.
Cyber Resilience Act (VO (EU) 2024/2847)	EU	Hersteller/Anbieter	Verordnung	Sicher-by-Design, Schwachstellenmanagement, Update-Pflichten für „Produkte mit digitalen Ele-menten“ → Anforderungen an SW-Liefer-kette/OSS-Compliance im OSiP-Ecosystem.

II. IT-Sicherheitsrecht (Bund und Bund-Länder-Kooperation)

Gesetz/ Regelungs-bereich	Normgeber	Vollzug/Ausführung	Verwaltungsform	Besondere Hinweise (Implikationen für Architek-tur/Betrieb)
Art. 91c GG IT-Staatsvertrag	Bund Bund/Länder	IT-PLR-Beschlüsse verbindlich für Bund/Länder	Verfassung/Staatsver-trag	Die Beschlüsse des IT-Planungsrats setzen bundes-weit verbindliche Architektur- und Sicherheitsstan-dards. Am 26.03.2025 wurde die Föderale IT-Archi-tekturrichtlinie, Version 1.9.0 (Beschluss 2025/17) beschlossen; sie verankert u.a. AV-08 „Sicherheit & Schutz". OSiP hat diese Vorgaben zu berücksichti-gen.
Leitlinie Informati-onssicherheit (IT-PLR, 2018)	IT-Planungsrat	Bund-/Länder-Verwaltungen; Kommunen Empfehlung	Beschluss	Mindestanforderungen: ISMS, sichere Netze, An-griffserkennung, Notfallmanagement → Pflichten in Verträgen mit Dritten zu verankern.
Nationale & Föde-rale IT-Architektur-richtlinie (Beschluss 2025/17)	IT-Planungs-rat/FIT-AB	Föderationsweit genutzte Systeme	Beschluss	AV-08 „Sicherheit & Schutz" (BSI-Standards, SDM, Geheimschutz) → verbindliche Vorgaben für OSiP-Zielarchitektur.
BSIG (inkl. Mindest-standards; künftige NIS2-Fassung)	Bund	BSI-Mindeststandards (Bund); KRITIS-Pflichten	Bundesgesetz	Die BSI-Mindeststandards sind für die Bundesver-waltung verbindlich und definieren u.a. Protokollie-rungs-, Detektions- und ISMS-Anforderungen; bei KRITIS-Relevanz kommen weitere BSIG/NIS-2-Pflichten hinzu. OSiP sollte Mindeststan-dards/Grundschutz als „Stand der Technik" abbil-den.
IT-NetzG (Verbin-dungsnetz	Bund	Betrieb Verbindungsnetz; Nut-zung durch Bund/Länder	Bundesgesetz	§ 3 Abs. 1 IT-NetzG schreibt den Datenaustausch Bund ↔ Länder über das Verbindungsnetz vor; im OZG-Anwendungsbereich bestehen eng begrenzte Ausnahmen (Front-Office). Für OSiP folgt daraus:

				direkte Anbindung an das Verbindungsnetz bzw. angeschlossene Verwaltungsnetze, mit Schutzbedarf „hoch“ und VS-NfD-geeigneter Ende-zu-Ende-Härtung (Ableitung aus Netzstrategie/BSI-Grundschutz, nicht Gesetzeswortlaut).
OZG & IT-Sicherheitsverordnung Portalverbund (ITSiV-PV)	Bund	Portalverbund; EfA-Rollen	Gesetz/VO	Die ITSiV-PV ist seit **20.01.2022** in Kraft und verweist auf Maßnahmen „nach dem Stand der Technik“ (u.a. BSI-Standards/Technische Richtlinien). Für exponierte Komponenten sind Pen-Tests/Web-Checks anzusetzen; OSiP muss diese Vorgaben abdecken.
UP Bund 2017 · Netzstrategie 2030 · ISR ITKB	Bund	Bundesverwaltung/ITKB	Verwaltungsvorschriften	Sie konkretisieren ISMS-Pflichten, Netzhärtung und Mindeststandards (z.B. Mindeststandard ISMS für IT-Konsolidierung Bund) und sind bei OSiP zu berücksichtigen.

III. IT-Sicherheitsrecht (Länder)

Land	Regelung
Baden-Württemberg	- **EGovG BW** (Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg) - **CSG** (Gesetz für die Cybersicherheit in Baden-Württemberg)
Bayern	- **BayDiG** (Gesetz über die Digitalisierung im Freistaat Bayern) - **BayDiV** (Verordnung über die Digitalisierung im Freistaat Bayern) - **BayCSS 2.0** (Bayerische Cybersicherheitsstrategie 2.0)

	- **ISMSR** (Richtlinie zur Förderung der Informationssicherheit durch Implementierung eines ISMS bei kommunalen Gebietskörperschaften) - **IKTSRBek** (Standards und Richtlinien für die Informations- und Kommunikationstechnik in der bayerischen Verwaltung) - **EVB-IT** (IT-Richtlinie für die bayerische Staatsverwaltung) - **BayVermKatG** (Bayerisches Vermessungs- und Katastergesetz) – hier: Regelung der informations- und kommunikationstechnischen Aufgaben in den öffentlichen Verwaltungen (Art. 12 Organisation).
Berlin	- **EGovG-BLN** (Gesetz zur Förderung des E-Government) - **ITDZAöRG BE** (Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin) - **eAktV Justiz** (Verordnung zur elektronischen Aktenführung bei den Gerichten und Staatsanwaltschaften im Land Berlin)
Brandenburg	- **BbgEGovG** (Brandenburgisches E-Government-Gesetz) - **ZIT-BB** (Erlass des Ministeriums des Innern zur Errichtung des Landesbetriebes „Brandenburgischer IT-Dienstleister“)
Bremen	- **BremDigG** (Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen – Digitalitätsgesetz) - **DataportStV** (Dataport Staatsvertrag) - **Bremische Cybersicherheitsstrategie 2023**
Hamburg	- **HmbITJG** (Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften der Freien und Hansestadt Hamburg) - **DataportStV** (Dataport Staatsvertrag)
Hessen	- **HITSiG** Hessisches Gesetz zum Schutz der Verwaltung (Hessisches IT-Sicherheitsgesetz) - **HesInfo-SichLL** (Informationssicherheitsleitlinie für die hessische Landesverwaltung) - **HCSS** (Hessische Cybersicherheitsstrategie)
Mecklenburg-Vorpommern	- **EGovG M-V** (E-Government-Gesetz Mecklenburg-Vorpommern)

	- **EAktVO M-V** (Verordnung zur elektronischen Aktenführung bei den Gerichten) - **IS-Leitlinie M-V** (Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern)
Niedersachsen	- **NDIG** (Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit) - **StVRDZPolTKÜ** (Staatsvertrag über die Einrichtung und den Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer) - **DataportStV** (Dataport Staatsvertrag) - **ISLL** (Leitlinie zur Gewährleistung der Informationssicherheit) - **ISLL-Justiz** (Informationssicherheitsleitlinie der niedersächsischen Justiz) - **ISRL IT-Mindestsicherheitsstandards** (Informationssicherheitsrichtlinie für technische Mindeststandards der IT-Sicherheit im Landesdatennetz) - **ISRL-Glossar** (Informationssicherheitsrichtlinie zur einheitlichen Begriffsdefinition im Informationssicherheitsmanagement des Landes Niedersachsen) - **ISRL-IT-Nutzung** (Informationssicherheitsrichtlinie für IT-Nutzung) - **ISRL-SchadSW** (Informationssicherheitsrichtlinie über die Abwehr von Schadsoftware) - **ISRL- ISi-Vorfälle** (Informationssicherheitsrichtlinie über den strukturierten Umgang mit Sicherheitsvorfällen) - **ISRL-Konzeption** (Informationssicherheitsrichtlinie über die risikobasierte Konzeption der Informationssicherheit von Services, Fachverfahren und Sicherheitsdomänen) - **ISRL-Datensicherung** (Informationssicherheitsrichtlinie über die Datensicherung)
Nordrhein-Westfalen	- **EGovG NRW** (Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen) - **DigiSiVO** (Verordnung über die Durchführung digitaler und hybrider Sitzungen kommunaler Vertretungen (Digitalsitzungsverordnung))
Rheinland-Pfalz	- **EGovGRP** (E-Government-Gesetz Rheinland-Pfalz)

	- **VV-LL_IS** (Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Rheinland-Pfalz) - **Informationssicherheitsleitlinie für die Justiz des Landes Rheinland-Pfalz**
Saarland	- **IT-SiG-SL** (Informationssicherheitsgesetz Saarland) - **SaarIIT-DLZEG** (Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen) - **Leitlinie zur Informationssicherheit der Landesverwaltung des Saarlandes**
Sachsen	- **SächsISichG** (Sächsisches Informationssicherheitsgesetz) - **SaInfoSichJusVwV** (VwV Informationssicherheit Justiz) - **Informationssicherheitsleitlinie für den Sächsischen Landtag** - **SaIS-SMF-VwV** (VwV Informationssicherheit SMF)
Sachsen-Anhalt	- **EGovG LSA** (Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt) - **JITG LSA** (Justiz-IT-Gesetz) - **DataportStVtr ST** (Dataport-Staatsvertrag) - **LISL LSA** (Informationssicherheitsleitlinie Sachsen-Anhalt)
Schleswig-Holstein	- **ITEG** (IT-Einsatz-Gesetz) - **EGovG** (Gesetz zur elektronischen Verwaltung für Schleswig-Holstein) - **DataportStV** (Dataport Staatsvertrag) - **Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein**
Thüringen	- **ThürEGovG** (Thüringer Gesetz zur Förderung der elektronischen Verwaltung)

IV. Zusammenfassung der Folgen für die Architektur

Bereich	Umsetzung
Netz & Anbindung	Direkte VN-Anbindung gem. IT-NetzG; für VS-NfD eine Ende-zu-Ende VS-taugliche Strecke (VSA-konform, inkl. Netzübergängen). Technische Segmentierung/Mandantierung Bund/Land/Justiz; Trennung von Transport-, Fach- und Betriebsdomänen.
Kryptografie & Transport	E2EE-Verschlüsselung der Inhaltsdaten; TLS nach BSI-Mindeststandard auf allen Transportstrecken; Härtung/Key-Management ohne Betreiber-Einsicht in Klartext.
ISMS & Nachweisführung	ISMS nach BSI-Standards (Grundschutz) mit Risiko-, Asset-, Patch-, Logging-/Detektions- und Incident-Prozessen; revisionsfeste Protokolle gemäß BSI-Mindeststandard „Protokollierung/Detektion" und VSA-Nachweisen (bei VS-Bezug).
Rollen & Zwecke	Strenges Rollen-/Rechte-Konzept; Zweckbindung/Datenminimierung technisch erzwungen; Rechtsgrundlagen-Profile je Verfahren/Land (inkl. Spezialnormen).
Verantwortlichkeitsmodell & Betrieb	Auftragsverarbeitung (Art. 28 DSGVO) als Zielmodell; Betreiber/FITKO ohne Inhaltszugriff (Zero-Trust/E2EE); klare Weisungs- und Schnittstellenregelung *versus* Fachverfahrensverantwortliche.
OZG/Antragsdienst	Für Bürger-/Unternehmens-Frontends OZG/ITSiV-PV beachten: ISMS-Pflicht, Pen-Test/Webcheck vor Anbindung, „Stand-der-Technik"-Maßnahmen; Transport-/Backoffice bleibt verwaltungsintern.
Interoperabilität & Standards	Orientierung an IT-PLR-Beschlüssen (Leitlinie Informationssicherheit, Föderale IT-Architekturrichtlinie); Nutzung von XÖV/OSCI/XTA; länderspezifische Formular-/Fristen-Profile konfigurierbar.
Geheimschutz	Bei SÜG/VS-Bezug VSA-konforme Prozesse (Einstufung/Kennzeichnung, Transport, Zugriff, Aufbewahrung); VS-IT-Eignung und Betriebs-/Monitoring-Nachweise; restriktive Weitergaben ausschließlich an öffentliche Stellen.
Personal & Zugriff auf VS-IT	Administrations-/Betriebsrollen an VS-IT gelten regelmäßig als sicherheitsempfindliche Tätigkeiten → Sicherheitsüberprüfung (SÜ), strikte Rollentrennung, Need-to-Know, Vier-Augen-Prinzip.
KRITIS/NIS2 (Betreiber)	Prüfung, ob Betreiber als (besonders) wichtige Einrichtung erfasst ist; dann Risikomanagement-, Melde-, Lieferketten- und Governance-Pflichten berücksichtigen.
Beschaffung/Zertifizierung	BSI-Grundschutz/ISMS-Zertifizierung als Regelfall; ITSiV-PV-Nachweise für Front-Office; EUCC/weitere Schemata perspektivisch berücksichtigen; VSA-Nachweise bei VS-Bezug.

Anlage 3

Regelungen der Länder zum materiellen Geheimschutz (Verschlusssachen)

Bundesland	Gesetz	Verwaltungsvorschrift	Bemerkung
Baden-Württemberg	SÜG BW	VSA BW	
Bayern	BaySÜG	VSA Bayern; VVBaySÜG	Die VSA ist alt (1995), die neuere VVBaySÜG verweist jedoch darauf.
Berlin	SÜG BE	VSA Berlin	Moderne VSA, die detaillierte und aktuelle Regelungen zu VS-IT (Abschnitt VIII), Abhörschutz (§ 41) und technischer Sicherung (§ 40) enthält und explizit auf BSI-Anforderungen verweist.
Brandenburg	BbgSÜG	VSA Brandenburg	
Bremen	BremSÜG	VSA Bremen	
Hamburg	HmbSÜGG	HmbVSA	
Hessen	HSÜVG	VSA Hessen	
Mecklenburg-Vorpommern	SÜG M-V	VSA M-V	
Niedersachsen	Nds. SÜG	VSA Niedersachsen	
Nordrhein-Westfalen	SÜG NRW	VSA NRW	
Rheinland-Pfalz	LSÜG	VSA RLP	
Saarland	SiÜpG	VSA Saarland	
Sachsen	SächsSÜG	VSA Sachsen	

Sachsen-Anhalt	SÜG LSA	VSA Sachsen-Anhalt	
Schleswig-Holstein	LSÜG	VSA Schleswig-Holstein	
Thüringen	ThürSÜG	VSA Thüringen	Konkrete Regelung zum elektronischen Schutz/Versand von VS in der VSA: § 21 Abs. 2 VSA: Versand von Verschlusssachen soll nach Möglichkeit nicht per Post, sondern über TK-Verbindungen nach § 40 VSA erfolgen (verschlüsselt). Zuvor sind Teilnehmerverzeichnisse zu kontrollieren; es ist ein Protokoll zu erzeugen. § 21 Abs. 3: VS, die mit einem BSI-zugelassenen Kryptosystem verschlüsselt wurden, bedürfen keines weiteren Schutzes. Dies gilt nicht für die Schlüssel; diese sind getrennt einzustufen und zu schützen. Nähere Informationen sind über das Amt für Verfassungsschutz zu beziehen. § 37: Produkte mit IT-Sicherheitsfunktionen zur Verwendung für Verschlusssachen müssen vom BSI zugelassen sein. § 40: Regelung zu Übertragung per TK-Verbindung (grundsätzlich verschlüsselt gemäß Vorgaben des BSI).

Anlage 4

1. Datenschutz- und Verfahrensrecht

Geltungs-bereich	Gesetz	Norm	Besonderheiten, die beim zentralen Betrieb zu beachten sind
EU	DSGVO	Art. 2 Abs. 2 lit. a, d DSGVO	Bereiche nationale Sicherheit/Strafjustiz sind *ausgenommen* → in den SÜG-Kontexten greift Spezial-/Landesrecht
Bund	BDSG	§ 1 Abs. 8 BDSG §§ 62-77 BDSG	OSiP-Anwendungsfälle im Bereich „nationale Sicherheit“: nach § 1 Abs. 8 BDSG ist die DSGVO hierfür entsprechend anwendbar; Fachgesetze schließen dies jedoch zum Teil aus (z.B. § 36 SÜG Bund) → in diesen Fällen sind die jeweiligen spezialgesetzlichen Datenschutzregeln abzubilden OSiP-Anwendungsfälle im Bereich „Strafverfolgung/-vollzug“: hier gilt nicht die DSGVO, sondern die – für den Bund – in §§ 45 ff. BDSG umgesetzte JI-Richtlinie; insbesondere sind die Anforderungen der §§ 62-77 BDSG abzubilden, z.B. besondere Regelungen für Übermittlung von Erkenntnissen (§ 74 BDSG)
Bund	SÜG (Bund)	u.a.: § 3 Abs. 1 a (organisatorische Trennung), § 21 (Übermittlung/Zweckbindung), § 22 (Löschung), § 36 (Selektive Anwendung BDSG/unabhängige Kontrolle)	§ 3 Abs. 1a: organisatorische Trennung § 21: Strenges Zweckbindungs-/Empfängerkreis-Regime § 22: definierte Aufbewahrungsfristen/Löschlogik § 36: Selektive Anwendung des BDSG → Rollen/Rechtekonzept; Policy-Enforcement und angepasstes Löschkonzept erforderlich
Baden-Württemberg	(SÜG BW)	§§ 19–24 (Sicherheits-/Sicherheitsüberprüfungsakte, Aufbewahrung, Datei-Verarbeitung, Übermittlung/Zweckbindung,	Detaillierte Akten-/Dateivorgaben, Zweckbindungen, Löschregeln; separates Regime für nicht-öffentl. Stellen → landspezifisches Löschkonzept/Prozesspfade

		Löschung); §§ 25–32 (nicht-öffentl. Stellen)	
Bayern	BaySÜG	Art. 29–32 (nichtöffentliche Stellen; Zuständigkeit; Sicherheitserklärung; Abschluss); Art. 5 Abs. 2 (Trennungsgebot)	enges Sonderregime für nichtöffentliche Stellen organisatorische Trennung → landesspezifische Rollen/Prozesse und Lösch-/Protokoll-Vorgaben
Berlin	SÜG BE	Trennungsvorgaben (insb. getrennte Aktenführung), Arten SÜ 1–3 (als Prozessrahmen)	organisatorische Trennung (zuständige Stelle ≠ Personalverwaltung), klare Akten-Trennung → strikte Rollentrennung im System.
Brandenburg	BbgSÜG	§§ 23–24 (Dateien/Zweckbindung); § 35 (Anwendung DSG/LDSG-Modifikationen)	ausdrückliche Datei-Regelungen und Zweckbindung; spezielle DSG/LDSG-Anwendung → Brandenburg-Profil (Policy-Mapping) erforderlich.
Bremen	BremSÜG	§§ 1-39	keine stark abweichenden materiellen Hürden in den SÜG-Regelungen (Vollzug über generelles Landesrecht)
Hamburg	HmbSÜGG	§ 3 Abs. 1 S. 2 (organisatorische Trennung von der Personalverwaltung); §§ 24–31 (Sonderregime nichtöffentlicher Stellen); § 36, § 36a (Anwendung HmbDSG/BDSG; unabhängige Datenschutzkontrolle)	organisatorische Trennung der zuständigen Stelle von der Personalverwaltung; eigenes, detailliertes Sonderregime für VS-Auftragnehmer; eigenständige Datenschutzaufsicht → Mandanten-/Rollenmodell und Protokollierung je Hamburg-Profil erforderlich
Hessen	HSÜVG	u.a. §§ 7–9 (SÜ-Arten/Verfahrenslogik)	prozessuale Besonderheiten (Anordnung nächsthöherer SÜ; Ausnahmen) → Steuerungslogik/Workflows müssen parametrisierbar sein

Mecklen-burg-Vor-pommern	SÜG M-V		
Nieder-sachsen	Nds. SÜG	(Datei-/Zweckbindungs- und Aktenregime in den §§ 15–21)	Eigene Datei-/Zweckbindung; Weiterverarbeitungstatbestände → landesspezifische Policies
Nordrhein-Westfalen	SÜG NRW	§ 4 Abs. 2 (Trennungsgebot: getrennt von Personalverwaltung, behördl. DSB, Korruptionsprävention); §§ 24–25 (Dateien; Übermittlung/Zweckbindung); §§ 38–39 (selektive BDSG-Verweisung mit Ausnahmen); § 40 (unabhängige Datenschutzkontrolle)	Besonders strenges Trennungsgebot + modifizierte Datenschutzlogik (BDSG-Selektivverweis, teils Ausschluss § 1 Abs. 8 BDSG) → saubere Tenant-/Routing-Trennung und Policy-Mapping notwendig
Rheinland-Pfalz	LSÜG	§§ 21–23, 26 (Zweckbindung, Löschung, Auskunft; nicht-öffentl. Stellen)	Definierte Löschfristen und Mitteilungspflichten ggü. Empfängern; Sonderregime nicht-öffentlicher Stellen → Aufbewahrung & landesspezifische Rollen/Tenants
Saarland	SiÜpG	§ 21 (Übermittlung/Zweckbindung); § 36–37 (Anwendung LDSG/VerfSchG; Aufsicht)	Zweckbindungs-Katalog inkl. Strafverwendungsschranken; eigene Aufsicht/Systematik Sachsen-Anhalt-Profil
Sachsen	SächsSÜG	§§ 8–9 (SÜ-Arten/Prozesslogik)	Prozessuale Feinheiten → parametrisierbare Prüffälle/Workflows

Schleswig-Holstein	LSÜG	Abschn. III–IV (Dateien/Zweckbindung; nicht-öffentl. Stellen)	Dokumentations- und Übermittlungspflichten; Strafverwendungsschranken → Logging/Policy-Checks je Land
Thüringen	ThürSÜG		

2. Organisations- und Fachrecht

Rechtsbereich	Gesetz	Norm	Potenzielle Hürden für zentralen Betrieb
Landes-E-GovG (z.B. EGovG NRW)	EGovG der Länder	Landesspezifische Vorgaben	Zwingende Vorgaben zur elektronischen Aktenführung und zu ISMS-Pflichten der Landesverwaltung. OSiP muss die Schriftgutverwaltung je Land anpassen können.
Länder-Hafensicherheit	z.B. BremHaSiG §§ 16 ff.; HaSiG NRW §§ 17 ff.; HmbHafenSG §§ 14 ff.; NHafenSG §§ 11 ff.	Detailvorgaben zur Datenverarbeitung/Protokollierung im Hafenkontext	Landes-spezifische Prozess-/Zuständigkeitslogik → OSiP-Profile je Hafenland.
Bundes-Fachrecht	LuftSiG; AtG; SprengG; GewO § 34a; WaffG § 5; BJagdG § 17; AufenthG § 73; StAG § 37; ProstSchG § 15	(jeweils Datenverarbeitung/Übermittlung im Rahmen von Zuverlässigkeits-/Sicherheitsüberprüfungen)	Grundsätzlich bundeseinheitlich; föderale Unterschiede entstehen primär, wenn Landesrecht (LDSG-Verweisnormen, Ausführungsvorschriften) abweichend modifiziert oder spezielle Zuständigkeiten/Prozesse (v. a. Hafensicherheit, Justizvollzug) anordnet.

Anlage 5

Gewährleistungsziele und technische/organisatorische Maßnahmen (mit Referenzen BSI-Grundschutz, C5, SDM)

Gewährleistungs-ziel	Anforderung	Referenz
Datenminimierung	**Erstellung und Umsetzung eines Löschkonzepts** zur Festlegung und Einhaltung von Löschfristen (Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO).	SDM Baustein 60 "Löschen und Vernichten", M60.P03 (P) BSI-Grundschutz CON.6.A1 (B)
	Regelung für die Löschung und Vernichtung von Informationen auf Datenträgern.	BSI-Grundschutz CON.6.A1 (B)
	Technische Systeme zur automatisierten Löschung nach Ablauf der Speicherfrist.	SDM Baustein 60 "Löschen und Vernichten" M60.P09 (P, D)
Verfügbarkeit	**Einführung der SDM-Methodik** (als Basis zur Systematisierung der TOMs).	BSI-Grundschutz CON.2.A1 (B)
	Erstellung eines Datensicherungskonzepts zur Wiederherstellung von Daten.	BSI-Grundschutz CON.3.A6 (S) (CON.3.A1 (B) für Rahmenbedingungen)
	Regelmäßiges Testen der Datensicherungen, um die einwandfreie und zeitgerechte Wiederherstellbarkeit zu prüfen.	BSI-Grundschutz CON.3.A15 (B); BSI C5 OPS-08.
	Erstellung eines Notfallhandbuchs (inkl. Kommunikations-, Wiederanlauf- und Wiederherstellungsplänen).	BSI-Grundschutz DER.4.A1 (S).
	Schutz vor Schadprogrammen durch ein Konzept und den Einsatz von Schutzprogrammen, die mindestens täglich aktualisiert werden.	BSI-Grundschutz OPS.1.1.4.A1 (B) (Konzept); C5 OPS-05 (tägl. Aktualisierung).
	Spezifizierung der Leistungsanforderungen und frühzeitiges Beheben von Ressourcenengpässen (Belastbarkeit).	BSI-Grundschutz APP.4.3.A11 (S); C5 OPS-03 (Kapazitätsmanagement).

Integrität	**Festlegung eines Rollen- und Berechtigungskonzepts** zur Einschränkung von Schreib- und Änderungsrechten.	C5 IDM-01 (Basiskriterium); SDM Baustein 51 "Zugriffe regeln", M51.P02 (P).
	Implementierung technischer Zugriffsrechtesysteme zur Umsetzung des Berechtigungskonzepts, um unbefugte Änderungen zu verhindern.	SDM Baustein 61 "Berichtigen", M61.S04 (P, D).
	Einsatz von Prüfsummen oder digitalen Signaturen zur Sicherstellung der Datenintegrität (insbesondere bei Übertragung und Speicherung von hochsensiblen Daten/Beweiswerterhalt).	BSI-Grundschutz CON.7.A16 (H); BSI-Grundschutz OPS.1.2.2.A5 (B).
	Regelmäßiger Soll-Ist-Vergleich der Konfigurationen zur Gewährleistung der Konzepteinhaltung und Richtigkeit.	BSI-Grundschutz OPS.1.1.1.A8 (S).
	Trennung von Entwicklungs- und Produktivsystemen.	BSI-Grundschutz OPS.1.1.6.A7 (B); BSI-Grundschutz SYS.1.7.A33 (H) (z.B. für z/OS).
Vertraulichkeit	**Verschlüsselung der Daten** bei Speicherung und Übertragung (angemessen zum Schutzbedarf).	BSI-Grundschutz CON.1 Kryptokonzept; OPS.2.3.A23 (H).
	Verwendung starker kryptografischer Verfahren (z.B. RSA-2048 Bit oder höher).	BayLDA Good Practice; C5 CRY-01 (Ergänzende Informationen).
	Sichere Übertragungsverfahren wie Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik.	SDM Baustein 61 "Berichtigen", M61.S11 (P, D).
	Regelungen für die Einrichtung und Löschung von Benutzenden und eindeutige Zuordnung jeder Kennung zu einer Person.	BSI-Grundschutz ORP.4.A1 (B).
	Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen (z.B. Administratoren) durch Mehr-Faktor-Authentisierung (MFA).	BSI-Grundschutz ORP.4.A10 (S).
	Zugangssicherung administrativer Schnittstellen durch Beschränkung auf dedizierte Systeme und idealerweise Zwei-Faktor-Authentisierung.	BSI-Grundschutz OPS.1.1.2.A16 (S).

	Sicherstellung des Zugriffs- und Zutrittsschutzes auf IT-Systeme und die Verarbeitungsumgebung (z.B. gesicherte Räume für IT-Komponenten).	BSI-Grundschutz CON.11.1.A14 (B); BSI-Grundschutz OPS.1.2.2.A3 (B).
Nichtverkettung	**Durchführung und Dokumentation von Zweckbeschreibung, Zwecktrennung und Zweckbindung** der Daten.	SDM Baustein 50 "Trennen", M50.D01 (P).
	Prüfung der Rechtsgrundlage für jede Datenübermittlung zwischen verschiedenen Mandanten oder Zwecken.	SDM Baustein 50 "Trennen", M50.D02 (P); M50.P08 (P).
	Sicherheitstechnische Isolation der Mandanten oder Verarbeitungen, insbesondere bei gemeinsam genutzter Infrastruktur.	SDM Baustein 50 "Trennen", M50.S03 (P, D, C).
	Getrennte Benutzerkennungen und Systeme zur Berechtigungsvergabe für Mandanten.	SDM Baustein 50 "Trennen", M50.S04 (P, D) und M50.S05 (P).
Transparenz	**Erstellung eines Protokollierungskonzepts** zur Gewährleistung der Rechenschaftspflicht und Evaluierbarkeit.	SDM Baustein 43 "Protokollieren" (Kapitel 2).
	Protokollierung aller sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen.	BSI-Grundschutz OPS.1.1.5.A3 (B).
	Speicherung der Protokollierungsdaten an einer zentralen Stelle (Logserver-Verbund).	BSI-Grundschutz OPS.1.1.5.A6 (S); SDM Baustein 43, M43.P06 (P).
	Einhaltung rechtlicher Rahmenbedingungen beim Protokollieren (insbesondere DSGVO und Löschfristen).	BSI-Grundschutz OPS.1.1.5.A5 (B).
	Zeitsynchronisation aller protokollierenden IT-Systeme (B).	BSI-Grundschutz OPS.1.1.5.A4 (B).
	Dokumentation der Wirksamkeit der ergriffenen Schutzmaßnahmen (Nachweisfähigkeit).	SDM Baustein 42 "Dokumentieren", M42.P29 (P).
Intervenierbarkeit	**Bereitstellung von Formularen und Prozessen** zur Beantragung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung).	SDM Baustein 61 "Berichtigen", M61.P11 (P); SDM Baustein 62 "Einschränken...", M62.P02 (P).

	Sicherstellung der unverzüglichen Bearbeitung von Anträgen innerhalb der gesetzlichen Fristen.	SDM Baustein 61 "Berichtigen", M61.P15 (D, C); SDM Baustein 62 "Einschränken...", M62.P07 (P, D, C).
	Prozess zur Identitätsprüfung von Antragstellern (zur Wahrnehmung von Betroffenenrechten).	SDM Baustein 61 "Berichtigen", M61.P14 (D, C); SDM Baustein 62 "Einschränken...", M62.P05 (P, C).
	Standardisierter Prozess zur Steuerung von Berichtigungsvorgängen.	SDM Baustein 61 "Berichtigen", M61.P03 (P).
	Prozess zur Dokumentation aller Berichtigungsvorgänge.	SDM Baustein 61 "Berichtigen", M61.P04 (D).

Anlage 6

Landesrechtliche Zustimmungsgesetze zum IT-Staatsvertrag (Art. 91c GG)

Land	Ratifizierung des IT-Staatsvertrages
Baden-Württemberg	Gesetz zum Vertrag zur Ausführung von Art. 91c GG (IT-Staatsvertrag), GBl. S. 314 f. vom 16. März 2010
Bayern	Bekanntmachung des IT-Staatsvertrags, GVBl. 2010, S. 139–144 (Bekanntmachung vom 15.03.2010); zusätzlich: Gesetz zum Zweiten IT-Änderungs-Staatsvertrag, GVBl. 2024, S. 66
Berlin	Gesetz zum IT-Staatsvertrag, GVBl. 2010, S. 121–132 (Gesetz vom 03.03.2010); Gesetz zum Zweiten IT-Änderungs-Staatsvertrag, GVBl. 2024, S. 552 (Gesetz vom 16.11.2024)
Brandenburg	Gesetz zum IT-Staatsvertrag, GVBl. I/10, Nr. 9 (2010); Gesetz zum Zweiten IT-Änderungs-Staatsvertrag vom 26.04.2024, GVBl. I/24, Nr. 16.
Bremen	Gesetz über den Staatsvertrag (IT-Staatsvertrag), Brem.GBl. 2010, S. 13 (Gesetz vom 22.12.2009)
Hamburg	Gesetz zum IT-Staatsvertrag, HmbGVBl. 2010, S. 200 (vom 16.02.2010)
Hessen	Gesetz zu dem Vertrag zur Ausführung von Art. 91c GG (GVBl. I 2010 S. 65) vom 4. März 2010
Mecklenburg-Vorpommern	Gesetz zum Vertrag zur Ausführung von Art. 91c GG (GVOBl. M-V 2010 S. 145) vom 11. März 2010
Niedersachsen	Gesetz zum IT-Staatsvertrag (Nds. GVBl 2010 S. 142); Erster IT-Änderungs-StV (Nds. GVBl 2019 S. 143) vom 17. März 2010, bzw. 20. Juni 2019
Nordrhein-Westfalen	Bekanntmachung des Staatsvertrages (GV. NRW. 2010 S. 9) vom 30. Dezember 2009; Bekanntmachung des Inkrafttretens vom 30. März 2010 (GV. NRW. 2010 S. 236)
Rheinland-Pfalz	Landesgesetz zu dem IT-Staatsvertrag (GVBl 2010 S. 36) mit Anlage (Vertrag) vom 19. Februar 2010
Saarland	Gesetz zu dem IT-Staatsvertrag (Amtsbl. 2010, S. 18) vom 10. Februar 2010

Sachsen	Gesetz zum IT-Staatsvertrag (SächsGVBl 2010 S. 43, vom 11.02.2010) vom 11. Februar 2010
Sachsen-Anhalt	Gesetz zum IT-Staatsvertrag (GVBl. LSA 2010 S. 142) vom 23. März 2010
Schleswig-Holstein	Gesetz zum IT-Staatsvertrag (GVOBl. 2010 S. 384); Gesetz zum Zweiten IT-Änderungs-StV (GVOBl 2024 S. 394, vom 29.04.2024) vom 19. März 2010 bzw. 29. April 2024
Thüringen	Thüringer Gesetz zu dem IT-Staatsvertrag (GVBl 2010 S. 21/22 – Zustimmung & Veröffentlichung) vom 8. Februar 2010

Anlage 7

Betreiber-Compliance-Checkliste für OSiP

I. Netz- und Architektur-Integrität

Anforderung	Erfüllungsnachweis
VN-Anschlusszwang	Die OSiP-Transportinfrastruktur und das Backend sind unmittelbar an das **Verbindungsnetz (VN**) angeschlossen. Nur das Front-Office (**OZG-Bereich**) ist vom Anschlusszwang ausgenommen.
Netzherrschaft	Die Netzanbindung erfolgt über ein gleichwertig gehärtetes Verwaltungsnetz. Die Netzherrschaft und die Kontrolle über das Routing müssen bei der öffentlichen Hand verbleiben.
Segmentierung/Mandantenfähigkeit	Logische und technische Segmentierung muss die Mandanten-/Ländertrennung (Daten, Nutzer, Prozesse) mit nachweisbarer Netzflusskontrolle (z.B. Firewall-Policies) gewährleisten.
Sicherheitsgefälle/Härtung	Der Netzverkehr erfolgt entlang des Sicherheitsgefälles. Betriebssysteme und Komponenten sind nach BSI-Standards gehärtet; Schwachstellenmanagement (CVSS-basiert) ist etabliert. Regelmäßige Penetrationstests und Patch-Fenster sind dokumentiert

II. Informationssicherheit & Zertifikate

Anforderung	Erfüllungsnachweis
ISMS-Basis	Ein wirksames ISMS nach ISO 27001 (mit Geltungsbereich des VN-TNA-Anschlusses) muss für alle relevanten Standorte und Prozesse vorgelegt werden.
Verwaltungsstandard	Das ISMS muss auf Basis des BSI-IT-Grundschutzes zertifiziert sein (idealerweise BSI-Zertifikat).

KRITIS-Compliance	Die KRITIS-Relevanz ist geprüft. Sofern einschlägig, sind die Nachweise gemäß § 8a BSIG bzw. den Vorgaben der NIS2-Richtlinie zu erbringen.
Subunternehmer-Transparenz	Eine vollständige Subunternehmer-Liste ist vorzulegen. Kontroll- und Weisungsrechte müssen vertraglich in die Sub-Kette gespiegelt werden (Back-to-Back-Klauseln).

III. Datenschutz und Kryptographie

Anforderung	Erfüllungsnachweis
Auftragsverarbeitung (AVV)	Ein Auftragsverarbeitungsvertrag (Art. 28 DSGVO) mit klaren TOMs, Datenminimierung und Zweckbindung muss abgeschlossen werden.
E2EE-Verschlüsselung	Ende-zu-Ende-Verschlüsselung (E2EE) der Inhaltsdaten ist für den Transportpfad zwischen Länderendpunkten und OSiP-Backend zwingend zu gewährleisten.
Schlüsselherrschaft	Die Hoheit über kryptografische Schlüssel muss allein bei der Verwaltung (FITKO/Länder) liegen. Kein exklusiver Providerzugriff auf die Schlüssel (kein Key-Escrow).
Datenschutz-Konformität	Privacy by Design/Default ist zu dokumentieren. Die DSFA-Unterstützung und die Meldeprozesse (Art. 33/34 DSGVO) sind im AVV festzulegen.
Drittlandtransfer	Die Datenlokation muss primär EU/EWR sein. Übermittlungen/Zugriffe aus Drittländern sind technisch zu unterbinden oder durch geeignete Art. 44 ff.-Garantien (z.B. Standardvertragsklauseln + ergänzende TOM) abzusichern.

IV. Governance, Exit und Vorsorge

Anforderung	Erfüllungsnachweis

Incident-Governance	Zentral auswertbares Logging/Monitoring und eine stringente Incident-Governance (Leitkoordination, 72-Stunden-Frist, Forensik-Pflicht) sind zu verankern.
Exit-Fähigkeit	Ein verbindlicher Exit-Plan muss Portabilität und Wechselmöglichkeit ohne Vendor-Lock-in sicherstellen (Datenexport in offenen Formaten, verifizierbare Datenlöschung).
Haftung und Versicherung	Haftungscaps nur für einfache Fahrlässigkeit vereinbaren; unbeschränkte Haftung für Vorsatz/grobe Fahrlässigkeit. Nachweis einer belastbaren Cyber-/Datenschutzversicherung.
Personal	Rollen- und Berechtigungskonzept (Least Privilege). Sofern erforderlich, sind SÜG-Prüfungen/Ermächtigungen für Personal mit Zugriff auf klassifizierte Daten durchzuführen.

V. Sonderfall: Cloud-Betrieb

Anforderung	Erfüllungsnachweis
C5-Testat	Vorlage eines aktuellen BSI-C5:2023-Prüfattests (Typ 2) des relevanten Cloud-Stacks.
BSI-Mindeststandard	Vertragliche Verpflichtung zur Umsetzung des BSI-Mindeststandards „Externe Cloud-Dienste“.
Cloud-Souveränität	BYOK/EKM (Bring Your Own Key / External Key Management) oder gleichwertiges Modell zur staatlichen Schlüsselhoheit muss gewährleistet sein.
DVC-Einbettung	Der Dienst muss die DVC-Konformitätskriterien (z.B. Nutzung offener Standards) erfüllen, um die Einbettung in die föderale Cloud-Governance zu ermöglichen.