

Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung

Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung

Impressum

Herausgeber

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3

60594 Frankfurt am Main

E-Mail: poststelle@fitko.de

Anstalt des öffentlichen Rechts | Präsidentin: Dr. Annette Schmidt

Ansprechpartner

Referat DG II 2 „Digitale Souveränität für die IT der öffentlichen Verwaltung“

Bundesministerium des Innern, für Bau und Heimat

Postanschrift: Alt-Moabit 140, 10557 Berlin

Hausanschrift: Salzufer 1 (Zugang Englische Straße), 10587 Berlin

E-Mail: DGII2@bmi.bund.de

www.cio.bund.de

Stand

Januar 2021

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Inhaltsübersicht

| | |
|--|---------------|
| Zusammenfassung | - 1 - |
| 1 Einführung | - 2 - |
| 2 Abgrenzung und Einordnung | - 4 - |
| 3 Strategie | - 6 - |
| 3.1 Strategische Ziele | - 6 - |
| 3.2 Lösungsansätze | - 7 - |
| 4 Umsetzung | - 12 - |
| 4.1 Maßnahmen zur Umsetzung der Lösungsansätze | - 12 - |
| 4.2 Governance | - 16 - |
| 5 Ausblick | - 18 - |
| 6 Anhänge und Verzeichnisse | - 19 - |
| 6.1 Ableitung der Lösungsansätze aus den Handlungsfeldern des Eckpunktepapiers | - 19 - |
| 6.2 Abbildungsverzeichnis | - 20 - |
| 6.3 Abkürzungsverzeichnis..... | - 21 - |

Zusammenfassung

In der Informationstechnik (IT) der Öffentlichen Verwaltung bestehen hohe - zum Teil kritische - Abhängigkeiten zu einzelnen Technologieanbietern. Dies birgt die Gefahr, die Kontrolle über die eigene IT zu verlieren und u. a. Informations- und Datenschutz gemäß nationalen und EU-weit gültigen Vorgaben nicht mehr gewährleisten zu können. Digitale Souveränität wird hier definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“¹. Im Rahmen der Fortschreibung des Eckpunktepapiers zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung verständigen sich Bund, Länder und Kommunen auf drei strategische Ziele: I. Wechselmöglichkeit, II. Gestaltungsfähigkeit sowie III. Einfluss auf Anbieter. Acht zugehörige Lösungsansätze sollen bei der Zielerreichung helfen. Die gemeinsame *Arbeitsgruppe (AG) Cloud Computing und Digitale Souveränität* definiert für jeden Lösungsansatz konkrete Maßnahmen und bearbeitet diese bzw. unterstützt bei der Umsetzung (vgl. Abbildung 1). Die Maßnahmen werden kontinuierlich durch Bund, Länder und Kommunen weiterentwickelt.

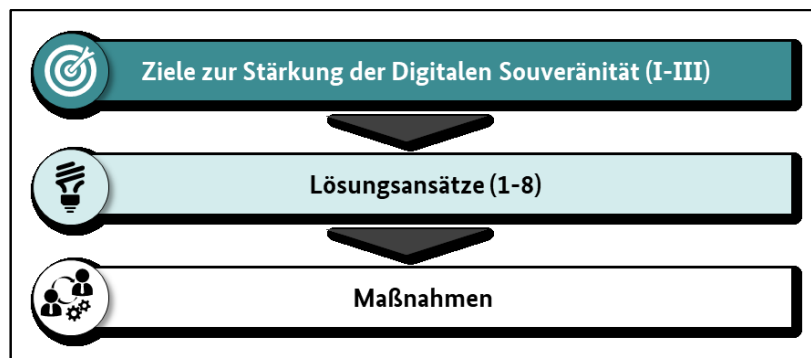


Abbildung 1: Zusammenhang der strategischen Ziele, Lösungsansätze und Maßnahmen

¹ Definition gemäß Studie zum Thema „Digitale Souveränität“ der Kompetenzstelle Öffentliche IT (ÖFIT).

1 Einführung

Bund, Länder und Kommunen haben sich zum Ziel gesetzt, die Digitale Souveränität der Öffentlichen Verwaltung zu wahren und kontinuierlich zu stärken. Mit Einrichtung der *AG Cloud Computing und Digitale Souveränität* durch den IT-Planungsrat (29. Sitzung des IT-Planungsrats am 27. Juni 2019, Entscheidung 2019/38) als länderoffene Arbeitsgruppe unter Federführung Nordrhein-Westfalens und des Bundes (vertreten durch das BMI) mit Vertretungen aus Spitzenverbänden der Kommunen und des Datenschutzes wurde ein grundlegender Rahmen zur Koordination des Vorhabens zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung in Deutschland geschaffen. Mit der Entscheidung zum Beschluss des *Eckpunktepapiers zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung*² im IT-Planungsrat (31. Sitzung am 25. März 2020; Entscheidung 2020/07) hat die Öffentliche Verwaltung in Deutschland zudem „die große strategische Bedeutung [der Stärkung der Digitalen Souveränität] für die Verwaltung“³ betont.

Die COVID-19-Pandemie verdeutlicht die Rolle von IT als kritische Infrastruktur. Die EU stellt in diesem Zuge Milliarden-Investitionen für u. a. digitale Infrastrukturen⁴ bereit, diskutiert Digitale Souveränität als ein Schwerpunkt in der deutschen EU-Ratspräsidentschaft⁵ und unterstreicht weiterhin die besondere Relevanz des Vorhabens: „Um den wirtschaftlichen Erfolg Europas und damit seine Handlungsfähigkeit auch zukünftig zu sichern, muss Europa sowohl technologisch als auch digital souverän werden“⁶. Kurzfristig eingesetzte digitale Lösungen zur Krisen- oder Folgenbewältigung müssen mit Normen und Werten von Deutschland und der EU, beispielsweise hinsichtlich Informationssicherheit oder Datenschutz, übereinstimmen. In der Entscheidung über den Einsatz – vorübergehend günstiger – Cloud-Lösungen muss Digitale Souveränität als ein Kriterium berücksichtigt werden.

In dem gemeinsamen Eckpunktepapier verständigten sich Bund, Länder und Kommunen auf das Ziel der Stärkung der Digitalen Souveränität der IT der Öffentlichen Verwaltung sowie fünf Handlungsfelder zur Erreichung des Ziels:

1. Strategische Analyse von Abhängigkeiten und vergleichbaren Vorhaben
2. Strategische Lösungskonzeption
3. Entscheidung und Umsetzungsbegleitung
4. Koordination sowie Abstimmung zwischen Bund, Ländern und Kommunen
5. Austausch mit Expertinnen und Experten

² „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder“.

³ Vgl. Entscheidung 2020/07 - Cloud-Computing und digitale Souveränität der 31. Sitzung des IT-Planungsrats.

⁴ Siehe: „Europäischer Ablaufplan“, Europäische Kommission, Juli 2020.

⁵ Siehe: „Programm der deutschen EU-Ratspräsidentschaft“, Auswärtiges Amt, Juli 2020.

⁶ Regierungserklärung von Bundeskanzlerin Merkel, 18. Juni 2020.

Das vorliegende Strategiepapier schreibt das Eckpunktepapier fort. Dafür werden strategische Ziele konkretisiert sowie Lösungsansätze und Maßnahmen aus den Handlungsfeldern des Eckpunktepapiers abgeleitet.

2 Abgrenzung und Einordnung

Digitale Technologien und -Lösungen sind heutzutage für viele Akteure ein fester Bestandteil des täglichen Handelns und Entscheidens. Hauptakteure sind insbesondere die Öffentliche Verwaltung (Bund, Länder und Kommunen), die Gesellschaft (Bürgerinnen und Bürger) und die Wirtschaft (Unternehmen). Für die Öffentliche Verwaltung sind digitale Lösungen für alle Bereiche der Exekutive, wie insbesondere die IT der Verwaltung, Innere Sicherheit, Verteidigung⁷, Außenpolitik⁸, Mobilität und Verkehr⁹, Klimaschutz oder Gesundheit und Pflege, relevant. Digitale Lösungen lassen sich wiederum in einzelne technische Komponenten (z. B. Software, Hardware und Infrastruktur, Plattformen, Fachanwendungen) untergliedern. Diese bilden im Ganzen die Technologie-Landschaft. Je nach Akteur, Politikbereich und technischer Komponente sind unterschiedliche Fähigkeiten, Kenntnisse und (Wahl-)Möglichkeiten zur Stärkung der Digitalen Souveränität notwendig.

Die vorliegende Strategie legt den Fokus auf die **IT der Öffentlichen Verwaltung**. Unter diesen Bereich fallen alle digitalen Lösungen, welche für den Arbeitsplatz und Betrieb notwendig sind. Dafür muss mittel- und langfristig die gesamte Technologie-Landschaft¹⁰ iterativ auf kritische Abhängigkeiten untersucht werden¹¹ sowie geeignete Handlungsoptionen aufgezeigt bzw. Maßnahmen initiiert werden. Ebenso zu berücksichtigen sind weiterhin technologische Trends (z. B. Big Data, Künstliche Intelligenz, Blockchain), die von großer Relevanz für die IT der Öffentlichen Verwaltung sind¹².

Wie im Eckpunktepapier beschrieben, agiert die Öffentliche Verwaltung in verschiedenen Rollen: *„Bund, Länder und Kommunen setzen sich zum Ziel, die Digitale Souveränität der Öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von Digitalen Technologien gemeinsam und kontinuierlich zu stärken.“* Zur Berücksichtigung der drei Rollen müssen digitale Lösungen entlang ihrer gesamten Wertschöpfungs- bzw. Leistungskette betrachtet werden (Souveränitätsdimensionen¹³).

Diese Dimensionen beschreiben Digitale Souveränität in voller Ausprägung und dienen als Orientierung für die spätere Ableitung der strategischen Ziele der Öffentlichen Verwaltung.

⁷ Siehe beispielsweise: <https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710>; vgl. auch im Kontext digitale Souveränität das Eckpunktepapier „Ausbau der digitalen Souveränität im Geschäftsbereich BMVg“, BMVg Abteilung CIT.

⁸ Siehe beispielsweise: <https://www.auswaertiges-amt.de/de/newsroom/maas-zeit/2284728>

⁹ Siehe beispielsweise: <https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html>

¹⁰ Technologien umfassen im Kontext dieses Papiers sowohl Software als auch Hardware.

¹¹ Unter Beachtung bestehender Vorhaben, wie beispielsweise das „Rahmenprogramm der Bundesregierung für Forschung und Innovation 2021 - 2024“ zur Mikroelektronik, BMBF, 2020.

¹² Unter Beachtung der jeweiligen Strategiepapiere der Öffentlichen Verwaltung, wie beispielsweise die „Datenstrategie des Bundes“, „Strategie Künstliche Intelligenz der Bundesregierung“, „Blockchain-Strategie der Bundesregierung“ sowie vergleichbare Strategien von Ländern und Kommunen.

¹³ Siehe: „Digitale Souveränität als strategische Autonomie – Umgang mit Abhängigkeiten im digitalen Staat“, Kompetenzzentrums Öffentliche IT und Fraunhofer-Instituts für Offene Kommunikation FOKUS, 2020

Übersicht der referenzierten Souveränitätsdimensionen:

Nutzungssouveränität (Nutzer¹⁴): Die Dimension beschreibt den Zugang zu Fähigkeiten und Ressourcen, um digitale Technologien gemäß den eigenen institutionellen Anforderungen und Prioritäten erfolgreich, effizient und (rechts-)sicher nutzen zu können. Dafür muss dem Nutzer eine freie Auswahl aus leistungsfähigen, alternativen IT-Lösungen möglich sein. Die Auswahl erlaubt flexible Wechsellmöglichkeiten, wenn sich neue Anforderungen aus Nutzersicht ergeben oder neue negative Folgen von Abhängigkeiten von Technologieanbietern den Einsatz weiter einschränken. Die Institution, die eine IT Lösung einsetzt („Nutzer“) ist die verantwortliche Stelle im datenschutzrechtlichen Sinne. Daher müssen diese gerade auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Ebenso ist die gezielte Entwicklung von Anwender- / Nutzerkompetenzen notwendig, um alternative digitale Lösungen erfolgreich einsetzen zu können.

Forschungs-, Entwicklung-, Produkt- und Betriebssouveränität (Bereitsteller¹⁵): Die Dimensionen beschreiben die Entscheidungsfreiheit sowie die erforderlichen Ressourcen und Kenntnisse beim Aufgreifen und Fördern von Forschungsthemen, der Konzeption, Ausgestaltung und Umsetzung eines Produktes, der Entwicklung bzw. Anpassung von Software sowie dem Aufbau und Betrieb von sicheren, vertrauenswürdigen und resilienten digitalen Systemen. Für den Bereitsteller muss die eigenständige Entwicklung, Inbetriebnahme und der Betrieb von IT-Lösungen unabhängig möglich sein. Der Bereitsteller muss in der Lage sein sich mit Herstellern am Markt rückkoppeln zu können, um Lösungen angemessen mitzugestalten (u. a. zur Gewährleistung des Datenschutzes und der Informationssicherheit). Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

Wissens- und Transparenzsouveränität (Auftraggeber¹⁶): Die Dimensionen beschreiben den freien Zugang zu Informationen und Wissen über Technologien sowie die Fähig- und Möglichkeiten Ressourcen, Systeme, Komponenten und Sachverhalte bewerten zu können. Für die Beauftragung digitaler Lösungen muss der Auftraggeber auf mehrere wettbewerbsfähige Anbieter zurückgreifen und Einfluss auf die Gestaltung des Angebots am Markt nehmen können. Ferner muss der Auftraggeber verbindliche Rahmenbedingungen zur Digitalen Souveränität (u. a. Informationssicherheit und Datenschutz) gegenüber Technologieanbietern bei Beauftragung, Entwicklung, Inbetriebnahme und Betrieb von IT-Lösungen durchsetzen können.

¹⁴ „Nutzer“ im Sinne der einsetzenden Institution, nicht im Sinne des Endnutzers, verantwortet den Einsatz von IT-Lösungen zur Unterstützung der Arbeit der Behörde; Nutzer sind beispielsweise IT-Abteilungen der Behörde.

¹⁵ „Bereitsteller“ verantworten die Entwicklung, Inbetriebnahme und den Betrieb von IT-Lösungen und sind beispielsweise IT-Dienstleister der Öffentlichen Verwaltung.

¹⁶ „Auftraggeber“ verantworten die Beauftragung und Beschaffung neuer IT-Lösungen und sind beispielsweise die IT-Dienstleister und Beschaffungsstellen der Öffentlichen Verwaltung.

3 Strategie

Auf Basis der Rollen der Öffentlichen Verwaltung und Souveränitätsdimensionen (siehe Kapitel 2) werden im vorliegenden Dokument zunächst **strategische Ziele** abgeleitet (Kapitel 3.1). Anschließend werden zur Erreichung dieser Ziele **Lösungsansätze** aufgezeigt (Kapitel 3.2). Die strategischen Ziele und Lösungsansätze sind mit den bestehenden IT-Zielen¹⁷ und mit Zielen bestehender IT-Programme¹⁸ abzugleichen. Geltende IT-Sicherheitsstandards finden in den beschriebenen Zielen und Lösungsansätzen Anwendung.

3.1 Strategische Ziele

Damit die Öffentliche Verwaltung ihre Rollen als Nutzer, Bereitsteller und Auftraggeber wahrnehmen kann, werden drei strategische Ziele verfolgt.

- I. **Wechselmöglichkeit:** Die Öffentliche Verwaltung hat die Möglichkeit einer freien Wahl bzw. eines flexiblen Wechsels zwischen IT-Lösungen, IT-Komponenten und Anbietern. Dies bedeutet, dass leistungsfähige und erprobte Alternativen zur Verfügung stehen, um kurzfristige Produktwechsel zu ermöglichen¹⁹. IT-Architekturen, Beschaffungswege und Personalschulungen müssen darauf ausgelegt sein, ein Wechsel mit verhältnismäßigen Kosten und angemessenem Aufwand zu ermöglichen.
- II. **Gestaltungsfähigkeit:** Die Öffentliche Verwaltung hat die Fähigkeit ihre IT (mit-)gestalten zu können. Dafür verfügt sie über die notwendigen Kompetenzen sowie (Zusammen-)Arbeitsstrukturen, um IT-Lösungen zu verstehen und bewerten zu können sowie bei Bedarf deren (Weiter-)Entwicklungen bzw. deren Betrieb sicherzustellen²⁰.
- III. **Einfluss auf Anbieter:** Die Öffentliche Verwaltung kann ihre Anforderungen und Bedarfe (z. B. hinsichtlich Produkteigenschaften, Verhandlung und Vertragsgestaltung) gegenüber Technologieanbietern artikulieren und durchsetzen. Neben rechtlichen Vorgaben und Rahmenbedingungen umfasst dies u. a. die Option eines IT-Betriebs in Rechenzentren der Öffentlichen Verwaltung, die Berücksichtigung von Richtlinien zu Informationssicherheit und zum Datenschutz sowie den Einfluss auf Lizenzmodelle und die Produkt-Roadmap.

¹⁷ Neben den strategischen Zielen zur Stärkung der Digitalen Souveränität werden bestehende IT-Ziele von Bund und Ländern berücksichtigt (Ziele aus IT-Strategie der Bundesverwaltung 2017-2021 und Ziele der Nationalen E-Government Strategie [NEGS] des IT-Planungsrats).

¹⁸ Beispielsweise mit Standardisierungs- und Konsolidierungsbemühungen von Bund, Ländern und Kommunen.

¹⁹ Für solch eine „Dual-Vendor-Strategie“ geht es darum ein Rahmen zu schaffen, in dem möglichst viele Anbieter agieren können und einen vielfältigen Wettbewerb unterstützen.

²⁰ Die notwendige Wertschöpfungstiefe der Öffentlichen Verwaltung ist für die jeweilige technische Komponente zu bestimmen (z. B. basierend auf Kriterien, wie Relevanz, Wirtschaftlichkeit und Spezifität).

Mit diesen drei strategischen Zielen wird ein ganzheitlicher Ansatz zur Stärkung der Digitalen Souveränität verfolgt (**Hybridstrategie**). Beispielsweise kann je nach Situation der Wechsel zu einem alternativen Anbieter bzw. Produkt, die (Mit-)Gestaltung alternativer Produkte, die Beauftragung eines Anbieters oder ein Mix der genannten Aktionen der effektivste Weg zur Steuerung von Abhängigkeiten sein²¹.

3.2 Lösungsansätze

Zur Erreichung der strategischen Ziele werden mehrere Lösungsansätze aufgezeigt (vgl. Abbildung 2). Diese basieren auf den Ansätzen der Handlungsfelder des Eckpunktepapiers und werden im Folgenden konkretisiert und erweitert. Die illustrative Ableitung der Lösungsansätze aus den Handlungsfeldern ist im Anhang in Kapitel 6.1 dargestellt. Die spezifischen Maßnahmen der Lösungsansätze werden in Kapitel 4 beschrieben.

| Ziele | I | II | III |
|----------------|---|---|--|
| | Wechselmöglichkeit | Gestaltungsfähigkeit | Einfluss auf Anbieter |
| Lösungsansätze | 1. Vorausschauende Analyse und Steuerung von Abhängigkeiten | 3. Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen in der IT | 5. Kooperative Mitgestaltung von IT-Lösungen |
| | 2. Beschaffung bzw. Entwicklung alternativer IT-Lösungen | 4. Aufbau Digitaler Kompetenzen und Expertenwissen | 6. Gemeinsames Verständnis und Vorgehen |
| | | | 7. Rechtliche Vorgaben |
| | | | 8. Politische Steuerung |

Abbildung 2: Lösungsansätze zur Erreichung der strategischen Ziele

Im Folgenden wird beschrieben, wie jeder Lösungsansatz unterschiedlich zur Erreichung der strategischen Ziele beiträgt.

| | |
|---|--|
| <p>1. Vorausschauende Analyse und Steuerung von Abhängigkeiten</p> | <p>Beitrag:</p> <ul style="list-style-type: none"> Frühzeitige Identifikation und Analyse kritischer Abhängigkeiten und Lock-in-Effekte²² in der Technologie-Landschaft, Schaffung von Transparenz über Maßnahmen zur Reduktion von Abhängigkeiten. <p>Ansatz: Initiale Betrachtung der bestehenden Technologie-Landschaft und der IT-Trends (z. B. Cloud-Computing, Big Data, Internet der Dinge, Künstliche In-</p> |
|---|--|

²¹ Dabei sollte die Öffentliche Verwaltung bzw. die jeweilige(n) Bundes-, Länder- und Kommunalen-Verwaltung(en) ein möglichst einheitliches Vorgehen anstreben, um Standardisierungs- und Konsolidierungsbemühungen zu berücksichtigen.

²² „Lock-in-Effekt“ beschreiben die negativ empfundene Zwangsbindung, die es dem Kunden wegen entstehender Wechselkosten und sonstiger Wechselbarrieren erschwert, Produkt / Service oder Anbieter zu wechseln.

telligenz). Priorisierung der Betrachtungsgegenstände (z. B. ausgewählte Anbieter, Teile des Technologiestacks oder spezifische Technologien) und anschließend tiefgehende Analyse von negativen Folgen der Abhängigkeiten. Die Analyse beinhaltet die Beschreibung von Zielvorstellungen der Öffentlichen Verwaltung und möglichen Handlungsoptionen. Die Erreichung der Ziele wird transparent nachverfolgt, um die Wirksamkeit der Maßnahmen zur Reduktion von Abhängigkeiten sicherzustellen.

2. Beschaffung bzw. Entwicklung alternativer IT-Lösungen

Beitrag:

- Schaffung von und Diversifizierung mit leistungsfähigen und bedarfsgerechten (insbesondere Open-Source-basierten) IT-Lösungen,
- Förderung der flexiblen Auswahl- und Wechselmöglichkeiten zwischen IT-Lösungen.

Ansatz: Identifikation, Beschaffung und Einsatz alternativer IT-Lösungen in der Öffentlichen Verwaltung. Bei Bedarf Entwicklung notwendiger Alternativen unter Berücksichtigung der angestrebten Architekturprinzipien, wie Modularität, offene Standards und Schnittstellen (siehe Lösungsansatz 3). Ebenso müssen Erfolgsfaktoren (z. B. die Nutzerzentrierung zur Sicherstellung der Nutzerakzeptanz, Leistungsfähigkeit, Datenverfügbarkeit) berücksichtigt werden. Fokussiert wird ein vermehrter Einsatz von Open-Source-Software (OSS), d.h. Software, die offen und, abhängig von der gewählten Lizenz, frei von technischen oder juristischen Beschränkungen in Bezug auf die Nutzbarkeit ist. OSS fördert Wahlfreiheit, die Wiederverwendbarkeit von Code und Lösungen sowie die flexible Anpassung von Lösungen bzw. Transparenz über Veränderungen am Quellcode.^{23, 24, 25} Der Quellcode muss dabei in verständlicher Form²⁶ zur Verfügung stehen, sodass die Öffentliche Verwaltung bspw. die Weiterentwicklung des Codes und die Betreuung bedarfsweise neu ausscheiden kann.

²³ Siehe: Beschluss des IT-Planungsrates (Sondersitzung am 18. September 2020) zur Investition in die Onlinezugangsgesetz-Umsetzung unter dem Prinzip u. a. „Offene Standards und Open Source“.

²⁴ Siehe: „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen“, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 22. September 2020.

²⁵ Siehe: „Open Source Software Strategy 2020 – 2023“, Europäische Kommission, Oktober 2020.

²⁶ Der Quellcode muss so dokumentiert und strukturiert sein, dass Dritte ihn verstehen und weiterentwickeln können und es möglich ist aus dem gelieferten Quellcode die in Frage kommende Software zu kompilieren.

3. Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen in der IT

Beitrag:

- Senken von Wechselbarrieren zwischen IT-Lösungen, IT-Komponenten und Anbietern,
- Förderung der Wiederverwendbarkeit von Lösungen bzw. Komponenten,
- Reduktion von Eintrittsschwellen für Anbieter.

Ansatz: Ebenenübergreifende Definition und Etablierung modularer und herstellerunabhängiger IT-Architekturen sowie offener, freier Standards, Schnittstellen und offener Dateiformate. Diese Prinzipien sind mittel- und langfristig insbesondere bei der Entwicklung von IT-Lösungen im Zuge von IT-Programmen innerhalb der Öffentlichen Verwaltung zu berücksichtigen (z. B. Onlinezugangsgesetz-Umsetzung und Konsolidierungsvorhaben)²⁷. Ebenso müssen Fachverfahren mittel- und langfristig vom Client entkoppelt werden, aber in denselben Verwaltungsbearbeitungsprozess integrierbar bleiben (Prozessplattform-Ansatz). Des Weiteren wird eine aktive Beteiligung an nationalen (z. B. XÖV), europäischen bzw. internationalen Standardisierungsbemühungen angestrebt.

4. Aufbau Digitaler Kompetenzen und Expertenwissen

Beitrag:

- Selbstständige Bewertung von IT-Lösungen,
- Bei Bedarf (Weiter-)Entwicklung bzw. Betrieb von Lösungen,
- Transfer von Wissen und Erfahrungen aus vergleichbaren Vorhaben aus Verwaltung, Wirtschaft und Wissenschaft.

Ansatz: Aufbau und Bündelung von (IT-)Fachwissen und Kompetenzen. Klare Aufgabenteilung, z. B. in den Bereichen Softwareentwicklung, Beschaffung oder Betrieb sowie den Fachbereichen und dem Anforderungsmanagement. Förderung des (inter-)nationalen und ebenenübergreifenden Austauschs mit öffentlichen und privaten Interessengruppen, auch auf EU-Ebene, z. B. zur Identifikation von und zum Lernen aus vergleichbaren Vorhaben.

5. Kooperative Mitgestaltung von IT-Lösungen

Beitrag:

- Mitgestaltung von IT-Lösungen durch Zusammenarbeit mit verschiedenen Anbietern und (inter-)nationalen Akteuren,

²⁷ Digitale Souveränität muss in Standardisierungs- und Konsolidierungsvorhaben bzw. Programmen zur Nachnutzung von Lösungen zukünftig als eine Dimension im Zuge der Entscheidungsfindung über geeignete Partner und Technologieanbieter berücksichtigt werden. Entsprechende Kriterien sind zu erarbeiten und abzustimmen.

- Einbringen von Anforderungen und Bedarfen der Öffentlichen Verwaltung in den Technologiemarkt.

Ansatz: Ebenenübergreifende Intensivierung der Zusammenarbeit innerhalb der öffentlichen IT auf nationaler und europäischer Ebene zur Herstellung interoperabler und länderübergreifender Lösungen. Ebenso soll durch die Intensivierung der intersektoralen Zusammenarbeit eine stärkere Diversifizierung des Angebots von Anbietern erreicht werden. Dies umfasst insbesondere die stärkere Zusammenarbeit mit OSS-Communities, OSS-Anbietern, proprietären Anbietern und kleineren und mittleren Unternehmen (KMU). Die Mitgestaltung von IT-Lösungen wird insbesondere durch die Offenlegung des Quellcodes und Nutzung geeigneter OSS-Lizenzen zur Wiederverwendung bzw. gemeinsamen (Weiter-)Entwicklung gefördert²⁸.

6. Gemeinsames Verständnis und Vorgehen

Beitrag:

- Stärkung der Verhandlungsposition der Öffentlichen Verwaltung gegenüber Technologieanbietern,
- Vermeidung von Redundanzen bzw. Mehraufwand und Nutzen von Synergieeffekten in der Öffentlichen Verwaltung,
- Festlegung einer gemeinsamen Strategie zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung.

Ansatz: Regelmäßige Abstimmung und Festlegung von Zielen und Vorgehen zwischen Bund, Ländern und Kommunen. Teil dieses Vorgehens betrifft bei Bedarf die Beschaffungsbündelung und Festlegung von Verhandlungsstrategien unter Berücksichtigung der Wahrung von offenen Märkten auch für KMU. Sensibilisierung über die Kritikalität ungewünschter Abhängigkeiten und die Notwendigkeit zur Stärkung der Digitalen Souveränität bei Mitarbeitenden der Öffentlichen Verwaltung sowie politischen Entscheidungsträgern.

7. Rechtliche Vorgaben

Beitrag:

- Positionierung und Durchsetzung von Kernanforderungen der Öffentlichen Verwaltung gegenüber Technologieanbietern,

²⁸ Siehe: „Open Source Software Strategy 2020 – 2023“, Europäische Kommission, Oktober 2020.

- Schaffung eines klaren Aktionsraums und Rechtssicherheit für Anbieter und die Öffentliche Verwaltung.²⁹

Ansatz: Formalisierung von Anforderungen in Form klarer rechtlicher und regulatorischer Regelungen, z. B. für Entwicklung, Beschaffung, Nutzung und Betrieb von IT-Lösungen. Berücksichtigung der Anforderungen Digitaler Souveränität bei Beschaffung, Vergabe- und Vertragsgestaltung und Betrieb. In diesem Zuge ist der Schutz des geistigen Eigentums der Öffentlichen Verwaltung sicherzustellen. Zu prüfen ist die Verankerung entsprechender Grundsätze zur Stärkung der Digitalen Souveränität im Vergaberecht. Zu prüfen ist weiterhin, inwiefern die rechtliche Verankerung einer Bevorzugung von OSS bei gleichem Funktionsumfang und Wirtschaftlichkeit zu proprietären Lösungen möglich ist. Wesentliches Merkmal Digitaler Souveränität im Betriebsbereich ist die Option eines On-Premise-Betriebs in Rechenzentren der Öffentlichen Verwaltung.

8. Politische Steuerung

Beitrag:

- Positionierung der Ziele zu Digitaler Souveränität in nationaler und europäischer Digitalpolitik,
- Etablierung politischer Rahmenbedingungen zur Stärkung der Digitalen Souveränität auf nationaler und europäischer Ebene.

Ansatz: Priorisierung des Ziels zur Stärkung der Digitalen Souveränität in den politischen Agenden der Verwaltung bzw. den Koalitionsverträgen der Bundesregierung. Bereitstellung der notwendigen Mittel und Ressourcen (z. B. durch spezifische Förderprogramme). Einbindung der EU als strategischer Partner mit geteilten Werten und gemeinsamen Governance-Mechanismen.

²⁹ Hinweis: Sollten Technologieanbieter die Kernanforderungen der Öffentlichen Verwaltung derzeit nicht erfüllen, jedoch die Umsetzung der Kernanforderungen bis zu einem vereinbarten Zeitpunkt gewährleisten, ist eine Beauftragung grundsätzlich möglich.

4 Umsetzung

Die Umsetzung der Lösungsansätze erfolgt anhand verschiedener Maßnahmen (siehe Kapitel 4.1). Die vorgestellten Maßnahmen sind **nicht abschließend**. Kapitel 8 beschreibt die Zusammenarbeit zwischen Bund, Ländern und Kommunen.

4.1 Maßnahmen zur Umsetzung der Lösungsansätze

Die initiale Übersicht der Maßnahmen dient als Bezugsrahmen für die *AG Cloud Computing und Digitale Souveränität* sowie deren Unterarbeitsgruppen (UAG) und wird gemeinsam regelmäßig weiterentwickelt. Für die Weiterentwicklung der Maßnahmen können insbesondere die Erkenntnisse der zukünftigen Strategischen Marktanalysen dienen. Aufgrund hoher Dringlichkeit wurde in 2019 die initiale Marktanalyse zu Software-Anbietern³⁰ durch das BMI beauftragt. Auf Grundlage der dortigen Erkenntnisse wurden beispielsweise Maßnahmen, wie Proof of Concepts, OSS-Alternativlösungen sowie Verhandlungen entlang definierter Anforderungen an Anbieter initiiert. Zukünftig erfolgen weitere Analysen auf Grundlage der holistischen Übersicht der Technologie-Landschaft und der priorisierten Betrachtungsgegenstände.

Bund, Länder und Kommunen können über die UAG an der Erarbeitung der Maßnahmen mitwirken sowie Vorschläge für weitere Maßnahmen einbringen. Abbildung 3 gibt einen Überblick der aus den Lösungsansätzen abgeleiteten Maßnahmen. Details zu Maßnahmen (z. B. Akteure, Meilensteine) werden durch die AG und UAG in gesonderten Steckbriefen kontinuierlich gepflegt.

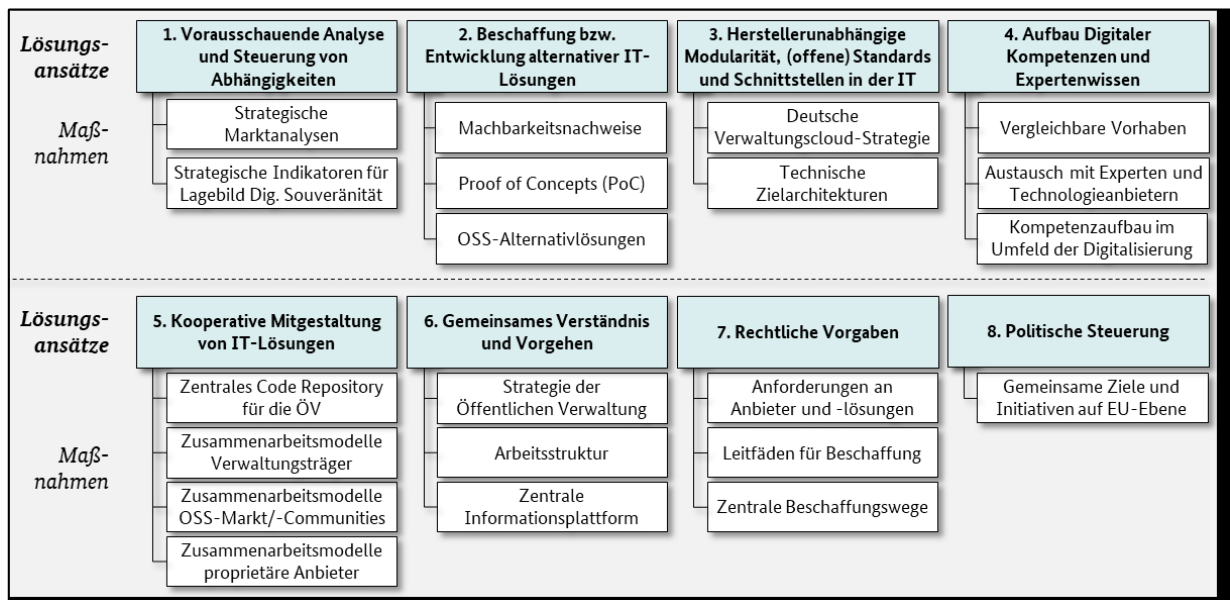


Abbildung 3: Maßnahmen zur Umsetzung der Lösungsansätze

³⁰ Siehe „Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern“, PwC Strategy& GmbH, 2019.

Im Folgenden werden die aktuellen Maßnahmen je Lösungsansatz vorgestellt.

1. Vorausschauende Analyse und Steuerung von Abhängigkeiten

- **Durchführung strategischer Marktanalysen zur Reduzierung von Abhängigkeiten:** Die initiale Marktanalyse *Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern* untersucht die negativen Folgen von Abhängigkeiten im Bereich Software und zeigt mögliche Handlungsoptionen auf. Derzeit wird ergänzend eine Marktanalyse im Bereich Datenbanken durchgeführt.
- **Erarbeitung strategischer Indikatoren für ein „Lagebild Digitale Souveränität“:** Bestimmung strategischer Indikatoren zur Messung des Fortschrittes und der Wirksamkeit des Vorhabens zur Stärkung der Digitalen Souveränität. Nutzung der Daten zur Aufbereitung einer ganzheitlichen Übersicht der Technologie-Landschaft der Verwaltung mit Informationen zu Abhängigkeiten, Schmerzpunkten und laufenden Gegenmaßnahmen. Der Aufbau einer holistischen Übersicht der Technologie-Landschaft ist die Basis zur Priorisierung weiterer Betrachtungsgegenstände für tiefergehende Analysen. Darauf basierend können in der Zuständigkeit der jeweils betroffenen Organisation operative (SMARTe) Ziele abgeleitet werden sowie deren Zielerreichung bzw. Umsetzung kontrolliert werden.

2. Beschaffung bzw. Entwicklung alternativer IT-Lösungen

- **Pflege der Übersicht der Machbarkeitsnachweise³¹ in der Öffentlichen Verwaltung:** Identifizierung bestehender alternativer (vorrangig OSS-basierter) IT-Lösungen und Pflege der Übersicht im Rahmen einer „Landkarte“ der Machbarkeitsnachweise³². Diese beinhaltet kritischen Erfolgsfaktoren aus Projekten mit alternativen IT-Lösungen und einen Überblick zu Erfahrungsbereichen der Öffentlichen Verwaltung. Mit Hilfe der „Landkarte“ soll der Einsatz alternativer Lösungen in Bund, Ländern und Kommunen vereinfacht werden.
- **Durchführung von Proof of Concepts (PoC):** Erprobung der Machbarkeit alternativer IT-Lösungen im Rahmen von PoC-Projekten zur Deckung des bestehenden Bedarfs. So sollen vor allem Lösungen getestet werden, zu denen noch kein ausreichender Machbarkeitsnachweis in der Öffentlichen Verwaltung besteht. Erste PoC-Projekte wurden bereits gestartet, z. B. im Bereich der Kollaborationsplattformen.
- **Förderung von OSS-Alternativlösungen:** Sicherstellung der Verfügbarkeit leistungsfähiger und skalierbarer Open-Source-Alternativlösungen sowie Forcierung des Einsatzes von OSS in der Öffentlichen Verwaltung. Die institutionalisierte Förderung von OSS-Lösungen ermöglicht u. a.

³¹ Ein Machbarkeitsnachweis wird definiert als ein Nachweis der technischen und organisatorischen Machbarkeit einer alternativen IT-Lösung.

³² Die aktuelle Version von August 2020 wurde am 03.09.2020 veröffentlicht: https://www.cio.bund.de/Shared-Docs/Kurzmeldungen/DE/2020/20200330_Machbarkeitsnachweise_download.pdf?_blob=publicationFile

eine verbesserte Ressourcenverteilung, mehr Wechselmöglichkeiten und einen verbesserten Einfluss auf die bedarfsgerechte Entwicklung von OSS.

3. Herstellerunabhängige Modularität, (offene) Standards und Schnittstellen in der IT

- **Konzeption der Deutschen Verwaltungscloud-Strategie (DVS) – Föderaler Ansatz³³:** Sicherstellung der Modularität, Kompatibilität und Interoperabilität von Cloud-Lösungen, um Austauschbarkeit bzw. Wiederverwendung zu ermöglichen. Für die Realisierung solch eines Föderalen Cloud-Verbunds werden in der DVS herstellerunabhängige, modulare Architekturen sowie ebenenübergreifende offene Standards und Schnittstellen (z. B. im Bereich Containerisierung) für Entwicklung, Inbetriebnahme und Betrieb von Cloud-Anwendungen in engen fachlichen Austausch mit bestehenden Entwicklungen und Aktivitäten³⁴ definiert.
- **Definition weiterer technischer Zielarchitekturen:** Erarbeitung weiterer Zielarchitekturen zur Reduktion identifizierter bzw. Vermeidung absehbarer Abhängigkeiten unter Berücksichtigung der Anforderungen der Öffentlichen Verwaltung (bei Bedarf unter Einbindung der Koordinierungsstelle für IT-Standards sowie weiteren bestehenden Entwicklungen und Aktivitäten). Für das jeweilige Anwendungsgebiet sollte jeweils eine Zielarchitektur definiert werden, die im Bereich Software vorzugsweise aus offenen OSS-Komponenten besteht und auch in der Industrie vorzugsweise Interesse findet, um von Netzwerkeffekten zu profitieren.

4. Aufbau Digitaler Kompetenzen und Expertenwissen

- **Identifikation und Austausch zu vergleichbaren (inter-)nationalen Vorhaben:** Der kontinuierliche Wissenstransfer und Erfahrungsaustausch mit vergleichbaren Vorhaben, insbesondere in der EU, dient der Ableitung von Erfolgsfaktoren und Best Practices.
- **Austausch mit Experten, Wissensträgern und Technologieanbietern:** Die Etablierung geeigneter Austauschformate (beispielsweise durch einen Expertenbeirat) ermöglicht die kontinuierliche Identifikation bestehender oder absehbarer Abhängigkeiten, möglicher Lösungen sowie potentieller Herausforderungen. Beispiele sind der Austausch mit Experten aus der Wissenschaft, mit Nichtregierungsorganisationen im Bereich Open Source oder mit ausgewählten Anbietern.
- **Kompetenzaufbau im Umfeld der Digitalisierung:** Aufbau der erforderlichen Kompetenzen zum Verstehen sowie zur Bewertung, Erforschung, Entwicklung, Betrieb oder zur Nutzung von Technologien. Die Aus-, Fort- und Weiterbildung der Öffentlichen Verwaltung (z. B. Fachkräfte-Ausbildungen, Studiengänge) muss dementsprechend angepasst bzw. erweitert werden. Die Er-

³³ Beschluss der Version 1.4.1 vom 17. November 2020 in der 33. Sitzung des IT-Planungsrats vom 23.10.2020

³⁴ U. a. Domäne öffentlicher Sektor in GAIA-X.

weiterung betrifft beispielsweise Berufsprofile im Bereich des Daten- und (agilen) Projektmanagements und sollte in diesem Zuge mögliche Verbesserungsvorschläge bzgl. der Tarif- und Anreizstrukturen im öffentlichen Sektor betrachten.

5. Kooperative Mitgestaltung von IT-Lösungen

- **Aufbau eines zentralen Code Repository für die Öffentliche Verwaltung:** Nutzung der Standards der DVS zum Aufbau eines Code Repository. Dazu zählen die Planung und Vorbereitung der mit einem Aufbau einhergehenden technischen, organisatorischen und rechtlichen Vorarbeiten (u. a. Auswahl einer geeigneten Trägerorganisation).
- **Konzeption von Zusammenarbeitsmodellen zwischen Verwaltungsträgern:** Identifizierung und Prüfung organisatorischer Grundlagen zur effizienten und wirksamen Zusammenarbeit innerhalb der Öffentlichen Verwaltung bei Lösungsentwicklungen (z. B. entsprechend FIT-Connect der FITKO).
- **Konzeption von Zusammenarbeitsmodellen mit OSS-Markt/-Communities:** Identifizierung und Prüfung von Möglichkeiten zur Einbindung des Open-Source-Marktes/-Communities zur Sicherstellung leistungs- und zukunftsfähiger Lösungen (z. B. durch Förderprogramme).
- **Konzeption von Zusammenarbeitsmodellen mit proprietären Anbietern:** Identifizierung und Prüfung von Möglichkeiten zur Einbindung proprietärer Anbieter zur Sicherstellung leistungs- und zukunftsfähiger Lösungen unter Wahrung der Anforderungen der Öffentlichen Verwaltung (z. B. durch einen kontinuierlichen Industriedialog).

6. Gemeinsames Verständnis und Vorgehen

- **Entwicklung einer Strategie der Öffentlichen Verwaltung:** Fortlaufende Abstimmung und Festlegung der gemeinsamen Ziele und eines gemeinsamen Vorgehens mit Bund, Ländern und Kommunen. Die strategischen Eckpunkte des Eckpunktepapiers werden durch die vorliegende Strategie konkretisiert.
- **Etablierung der Arbeitsstruktur in der AG Cloud Computing und Digitale Souveränität:** Zur Formalisierung und Förderung der Zusammenarbeit zwischen Bund, Ländern und Kommunen wurde eine Arbeitsstruktur der AG Cloud Computing und Digitale Souveränität mit fachlich fokussierten Unterarbeitsgruppen eingerichtet. Die Arbeitsergebnisse der UAG werden in die AG eingebracht; bei Bedarf bereitet die AG die Beschlussempfehlung für den IT-Planungsrat vor.
- **Aufbau einer zentralen Informationsplattform:** Konzeption einer Kommunikationsstrategie und Bereitstellung der Inhalte über eine Informationsplattform zur Förderung der Vernetzung zwischen Akteuren sowie zur Information und zur Sensibilisierung über Digitale Souveränität.

7. Rechtliche Vorgaben

- **Formulierung von Anforderungen an Technologieanbieter und -lösungen:** Definition von übergreifenden Anforderungen an die Beschaffung von Informations- und Kommunikationstechnik durch bzw. für die Öffentliche Verwaltung. Diese Anforderungen sollen die Abhängigkeit von einzelnen Anbietern reduzieren, indem sie einen Rahmen für IT-Leistungen und deren Anbieter für die Öffentliche Verwaltung bei der Entwicklung und Bereitstellung von Lösungen vorgeben.
- **Erstellung von Leitfäden für Beschaffung:** Ergänzung der konkreten Vorgaben hinsichtlich Digitaler Souveränität (u. a. zu Pflegeleistungen, Servicezeiten, Datenschutz) im Vergabeprozess, beispielsweise durch Ergänzung der bereits etablierten Musterformulare der EVB-IT³⁵ Verträge sowie Fortschreibung der UfAB³⁶.
- **Prüfung von zentralen Beschaffungswegen:** Identifikation und Sicherstellung von Möglichkeiten zur zentralen Beschaffung von alternativen Lösungen in der Öffentlichen Verwaltung. Ebenso soll eine Methodik entwickelt werden, wie ebenenübergreifende Bedarfe der Verwaltung erhoben und gebündelt werden können.

8. Politische Steuerung

- **Abstimmung gemeinsamer Ziele und Initiativen auf EU-Ebene:** Festlegung gemeinsamer Ziele zur Stärkung der Digitalen Souveränität. Initiierung gemeinsamer Initiativen zur Kooperation auf europäischer Ebene mit Deutschland in einer Vorreiterrolle. Vorschläge gemeinsamer Initiativen umfassen beispielsweise die Förderung offener digitaler Ökosysteme, die koordinierte Umsetzung der EU-Vorschriften für das öffentliche Beschaffungswesen, das Aufsetzen öffentlich-private Partnerschaften in den Bereichen KI, Daten und Robotik³⁷ oder die Einrichtung eines „Open Source Programm Office“³⁸.

4.2 Governance

Für die Umsetzung der Maßnahmen zur Stärkung der Digitalen Souveränität wird die Einbindung zahlreicher Akteure auf Ebene von Bund, Ländern und Kommunen angestrebt. Ausgangspunkt war die Einrichtung der *AG Cloud Computing und Digitale Souveränität* durch den IT-Planungsrat. Die konkrete inhaltliche Erarbeitung erfolgt im Rahmen der UAG³⁹ der *AG Cloud Computing und Digitale Souveränität*. Hierbei wird ein

³⁵ Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)

³⁶ Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB)

³⁷ Siehe: „Digital sovereignty for Europe“, Europäisches Parlament Think Tank, 2020

³⁸ Siehe: „Open Source Software Strategy 2020 – 2023“, Europäische Kommission, Oktober 2020.

³⁹ Bestehend aus 1) UAG Technik & Betrieb, 2) UAG Beschaffung und 3) UAG Kommunikation.

Informationsaustausch mit der Industrie, Experten der Privatwirtschaft und weiteren wichtigen Mitstreitern explizit angestrebt. Ergebnisse der UAG werden der AG zur Entscheidung vorgelegt. Die AG wird auf dieser Grundlage weitere Beschlussempfehlungen für den IT-Planungsrat vorbereiten. Organisatorische Details wurden im Papier zur *Arbeitsstruktur der AG Cloud Computing und Digitale Souveränität* beschlossen. Im Beschluss 2020/31 des IT-Planungsrats wurden Bund, Länder und Kommunen um die aktive Mitarbeit im Rahmen der festgelegten Arbeitsstruktur innerhalb der Unterarbeitsgruppen gebeten.

Zur Zielerreichung ist sowohl eine effektive Zusammenarbeit innerhalb der Öffentlichen Verwaltung in Deutschland als auch mit europäischen Mitgliedsstaaten, der Industrie und der Wissenschaft notwendig. Im weiteren Vorgehen ist durch die AG zu prüfen, wie die weitere institutionelle Verankerung und Governance des Themas Digitale Souveränität der Öffentlichen Verwaltung gestaltet werden kann (z. B. durch eine zentrale Trägerorganisation bzw. dezentrale Arbeitseinheiten).

5 Ausblick

Die skizzierten strategischen Ziele und Lösungsansätze bilden die Grundlage für die gemeinsame und kontinuierliche Stärkung der Digitalen Souveränität. Darauf aufbauend werden Maßnahmen (vgl. Kapitel 4.1) bearbeitet und regelmäßig weiterentwickelt. Die Detaillierung der jeweiligen Maßnahmen erfolgt gesondert in Steckbriefen der AG und UAG. Hierbei werden die relevanten Akteure und Zeitplanungen zur Umsetzung sowie eine ggf. notwendige, verbindliche Zeitplanung für die Einführung der Standards inklusive eines Migrationszeitraumes bestimmt. Ebenso werden neue Maßnahmen detailliert (z. B. auf Basis der Ergebnisse der Marktstudie im Bereich der Datenbanken).

Wesentliche nächste Schritte zu konkreten Maßnahmen umfassen:

1. Erarbeitung von Standards und Zielarchitekturen auf Grundlage der Deutschen Verwaltungscloud-Strategie (Beschluss in 33. Sitzung des IT-Planungsrats am 22. Oktober 2020),
2. Beschluss der Anforderungen an Technologieanbieter und -lösungen im IT-Planungsrat (voraussichtlich Mitte 2021),
3. Konzeption einer zentralen, koordinierenden Stelle zur Förderung von OSS in der Öffentlichen Verwaltung. In einem ersten Schritt soll geprüft werden, in welchen Bereichen Bedarf und Mehrwert für den Einsatz von OSS in der Öffentlichen Verwaltung besteht (insbesondere zur Reduktion, der in der Marktanalyse als kritisch bewerteten Abhängigkeiten im Bereich Arbeitsplatz).
4. Erarbeitung eines Gesamtbildes zur Stärkung der Digitalen Souveränität (vgl. Kapitel 4.1, Maßnahme „Strategische Indikatoren für Lagebild Digitale Souveränität“). In Anlehnung an das *Dashboard Digitalpolitik*⁴⁰ muss ein solches „Lagebild zur Digitalen Souveränität“ einen ganzheitlichen Überblick der Technologie-Landschaft der IT der Verwaltung geben. Mit Hilfe des „Lagebilds“ sollen die Analyse kritischer Betrachtungsgegenstände priorisiert und das systematische Durchleuchten der gesamten Technologie-Landschaft vereinfacht werden. Weiterhin muss Transparenz über den Fortschritt und die Wirksamkeit der Maßnahmen zur Stärkung der Digitalen Souveränität geschaffen werden. In einer weiteren Ausbaustufe sollte das „Lagebild“ die Bewertung neuer Technologien mit zukünftiger Relevanz für die IT der Verwaltung (z. B. Daten, Künstliche Intelligenz, Blockchain) einbeziehen. Ebenso sollte in einer späteren Ausbaustufe die politikfeldübergreifende Betrachtung und Berücksichtigung weiterer Akteure (z. B. aus den Bereichen Bildung, Industriepolitik, Verteidigungspolitik, Gesundheit, Mobilität) erfolgen.

⁴⁰ Siehe: „Digitalisierung gestalten“, Bundesregierung, 2020 (<https://www.digital-made-in.de/dmide>, 2020)

6 Anhänge und Verzeichnisse

6.1 Ableitung der Lösungsansätze aus den Handlungsfeldern des Eckpunktepapiers

An verschiedenen Stellen wird derzeit das Konzept der Digitalen Souveränität aufgegriffen und vorangetrieben. Die verschiedenen Beiträge greifen dabei naturgemäß jeweils einzelne Aspekte des sehr umfangreichen Themenkomplexes Digitale Souveränität heraus und betonen jeweils unterschiedliche Sichten. Dabei sind diese Beiträge als komplementär zu verstehen, außerdem bauen sie im Zeitverlauf aufeinander auf und entwickeln verschiedene Ansätze weiter, wobei die Kernaussagen erhalten bleiben.

Das Eckpunktepapier und die hier vorgelegte Strategie sind als Grundsatzpapier und dessen Weiterentwicklung hin zu einer Umsetzung angelegt. In den Handlungsfeldern (HF) des Eckpunktepapiers werden Ansätze zur Stärkung der Digitalen Souveränität beschrieben. Diese werden in der vorliegenden Strategie ausdifferenziert, erweitert und mit Maßnahmen hinterlegt (vgl. Abbildung 4). Dabei gibt es auch inhaltliche Weiterentwicklungen, und die HF werden unter neu formulierte bzw. geschärfte strategische Ziele subsumiert.

Handlungsfeld 1 wird erweitert, sodass neben der Analyse von Abhängigkeiten auch deren Steuerung (siehe Maßnahme „Lagebild“) betrachtet wird. Im Einklang mit der Verfolgung einer Hybridstrategie werden in der Strategischen Lösungskonzeption (Handlungsfeld 2) verschiedene technische, organisatorische und rechtliche Lösungsansätze zur Reduktion von kritischen Abhängigkeiten bzw. zur übergreifenden Stärkung der Digitalen Souveränität konkretisiert. Dort angesiedelte Maßnahmen unterteilen zumeist in einen konzeptionellen (Handlungsfeld 2) sowie einen Teil zur Entscheidung über den Einsatz der erarbeiteten Lösungen und Konzepte bzw. der Umsetzungsbegleitung (Handlungsfeld 3). Handlungsfeld 4 wird neben der kontinuierlichen Abstimmung zwischen Bund, Ländern und Kommunen um die politische Positionierung des Themas Digitale Souveränität auf nationaler und europäischer Ebene erweitert. Handlungsfeld 5 wird neben dem Austausch mit Experten um den kontinuierlichen Aufbau von Kompetenzen erweitert.

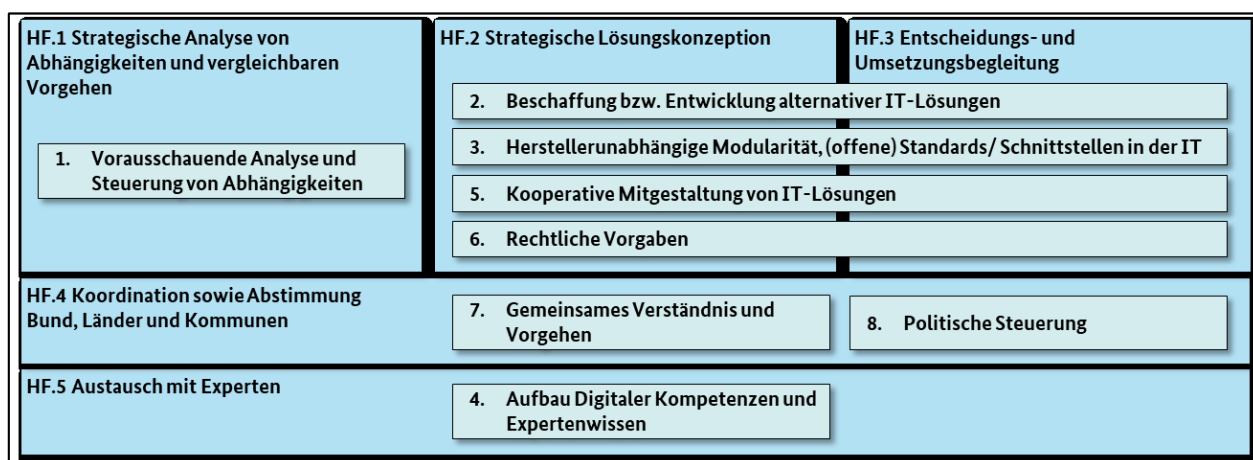


Abbildung 4: Ableitung der Lösungsansätze aus den Handlungsfeldern des Eckpunktepapiers

6.2 Abbildungsverzeichnis

| | |
|---|--------|
| Abbildung 1: Zusammenhang der strategischen Ziele, Lösungsansätze und Maßnahmen | - 1 - |
| Abbildung 2: Lösungsansätze zur Erreichung der strategischen Ziele | - 7 - |
| Abbildung 3: Maßnahmen zur Umsetzung der Lösungsansätze..... | - 12 - |
| Abbildung 4: Ableitung der Lösungsansätze aus den Handlungsfeldern des Eckpunktepapiers | - 19 - |

6.3 Abkürzungsverzeichnis

| | |
|---------------|---|
| AG | Arbeitsgruppe |
| BMBF | Bundesministerium für Bildung und Forschung |
| BMI | Bundesministerium des Innern, für Bau und Heimat |
| BMVg | Bundesministerium der Verteidigung |
| CIT | Cyber- und Informationsraum |
| DVS | Deutsche-Verwaltungscloud-Strategie |
| EPP | Eckpunktepapier |
| EU | Europäische Union |
| EVB-IT | Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen |
| FITKO | Föderale IT-Kooperation |
| HF | Handlungsfeld |
| IT | Informationstechnologie |
| KMU | Kleine und mittlere Unternehmen |
| KoSIT | Koordinierungsstelle für IT-Standards |
| OSS | Open-Source-Software |
| ÖV | Öffentliche Verwaltung |
| PoC | Proof of Concept (Machbarkeitsstudie) |
| UAG | Unterarbeitsgruppe |
| UfAB | Unterlage für Ausschreibung und Bewertung von IT-Leistungen |