Der Beauftragte der Bundesregierung für Informationstechnik

IT-Planungsrat

IT-Rat

Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung

Eckpunkte – Ziel und Handlungsfelder

- Version 1.0.1 vom 31. März 2020 –

Beschluss Nr.: 2020/01 des IT-Rats vom 24. März 2020
Beschluss Nr.: 2020/19 des IT-Planungsrats vom 04. Mai 2020

03/2020

Ausganglage und Motivation

Die zunehmende Digitalisierung verändert alle Arbeitsbereiche – auch die der Öffentlichen Verwaltung – umfassend und mit hoher Dynamik. Sie erbringt wichtige Ergebnisse, wie z. B. höhere Effizienz durch verbesserte Zusammenarbeit. Aufgrund des steigenden Grades an Vernetzung und Datenaustausch ist Digitalisierung z. B. in den Feldern Informationssicherheit oder Datenschutz auch mit Risiken verbunden.

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]. Eine solche Ausübung ist insbesondere für die Öffentliche Verwaltung zur Erfüllung ihrer hoheitlichen Aufgaben durch digitale Verwaltungsprozesse wichtig. Sofern die Digitale Souveränität nicht ausreichend gewahrt ist, kann die Handlungsfähigkeit eingeschränkt werden. Sie ist daher für die Öffentliche Verwaltung zentral und fortlaufend zu evaluieren sowie bei Entscheidungen zu berücksichtigen.

Verwaltungen bauen für ihre Informations- und Kommunikationstechnik (IKT) Geschäftsbeziehungen mit externen, meist privaten IT-Anbietern auf, die Abhängigkeiten verursachen können. Derartige Abhängigkeiten sind hinsichtlich möglicher Schmerzpunkte zu bewerten, um potentielle Beeinträchtigungen für die Digitale Souveränität der Öffentlichen Verwaltung auszuschließen oder mindestens einzuschränken. Die aktuell identifizierten Schmerzpunkte umfassen eingeschränkte Informationssicherheit, rechtliche Unsicherheit, unkontrollierbare Kosten, eingeschränkte Flexibilität und fremdgesteuerte Innovation.

Eine für den Beauftragten der Bundesregierung für Informationstechnik (BfIT) durchgeführte strategische Marktanalyse zur Untersuchung von Abhängigkeiten von Softwareanbietern in der Bundesverwaltung ergab konkrete Anhaltspunkte für Beeinträchtigungen der Digitalen Souveränität. Die Studie hat ein Rahmenwerk zur Bewertung von Abhängigkeiten und daraus resultierenden Schmerzpunkten erarbeitet. Fokus der folgenden initialen Anwendung des Rahmenwerks waren Bürosoftware, Desktop-Betriebssysteme und Server-Betriebssysteme[2], welche in der Folge auch auf andere Technologie[3]-Schichten auszuweiten ist. Auf den betrachteten Schichten identifiziert die Untersuchung durch Abhängigkeiten verursachte kritische Schmerzpunkte, insbesondere in der Informationssicherheit und der Gewährleistung datenschutzrechtlicher Vorgaben, welche die Selbstständigkeit, Selbstbestimmung und Sicherheit der Öffentlichen Verwaltung in der digitalen Welt beeinträchtigen können. Aufgrund der weiterhin ansteigenden IT-Anbieterkonzentration am Markt werden derartige Abhängigkeiten potentiell weiter zunehmen. Zusätzlich erhöhen technologische und geopolitische Trends, wie etwa angespannte Handelsbeziehungen oder der Umstieg auf Public Cloud-Lösungen, die Relevanz dieses Themas.

Zusammenfassend kann zunächst festgehalten werden, dass die Digitale Souveränität der Öffentlichen Verwaltung gestärkt werden muss. Gegenwärtige Entwicklungen bei den Angeboten von IT-Anbietern, insb.

[1] Definition gem. Studie zum Thema „Digitale Souveränität" der Kompetenzstelle Öffentliche IT (ÖFIT).

[3] Technologien umfassen im Kontext dieses Papiers sowohl Software als auch Hardware.

der Trend zu skalierbaren und effizienten Public Cloud-Lösungen, stehen der Digitalen Souveränität entgegen. Ebenso problematisch wirkt sich die herstellerseitige Verarbeitung von Metadaten und Daten zur Produktnutzung aus. Die identifizierten IT-Trends unterstreichen den Handlungsdruck zur Reduzierung bestehender Schmerzpunkte und Stärkung der Herstellerunabhängigkeit u. a. durch die Identifikation geeigneter Alternativen und die Stärkung der Wechselmöglichkeit und -fähigkeit durch offene Schnittstellen und Standards. Bund, Länder und Kommunen bestimmen mit den folgenden Festlegungen einen Handlungsrahmen, der gemeinsam verfolgt werden soll. Zentral ist dabei eine kontinuierliche Abstimmung verbunden mit transparentem Handeln.

Ziel

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.*

Handlungsfelder

Zur Erreichung des beschriebenen Ziels verständigen sich Bund, Länder und Kommunen auf die in Abbildung 1 dargestellten **Handlungsfelder.** Die Maßnahmen der Handlungsfelder werden zwischen Bund, Ländern und Kommunen gemeinsam koordiniert und abgestimmt, die Umsetzung erfolgt in der Zuständigkeit der jeweils betroffenen Organisation[4].

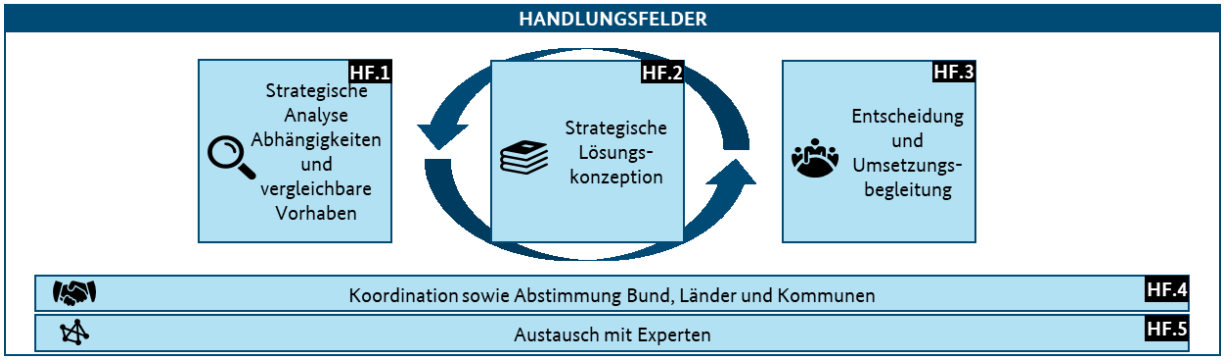

Abbildung 1: Überblick Handlungsfelder

HF.1: Strategische Analyse von Abhängigkeiten und vergleichbaren Vorhaben

Die seitens des BfIT veröffentlichte Studie mit dem Schwerpunkt auf einzelne Software-Schichten hat Schmerzpunkte aufgedeckt und stellt einen ersten Schritt für die kritische Auseinandersetzung mit IT-Anbietern durch die Öffentliche Verwaltung dar. Um die Digitale Souveränität der Öffentlichen Verwaltung kontinuierlich zu stärken, sollen Abhängigkeiten zu weiteren IT-Anbietern analysiert und vergleichbare Vorhaben zur Reduzierung von Schmerzpunkten evaluiert werden. Die Analysen sollen hierbei anhand von transparenten und einheitlichen Kriterien durchgeführt werden. Diese Kriterien werden gemeinsam mit

[4] Ein zu erarbeitenendes Rahmenwerk ermöglicht die Evaluierung der Ausprägung der Digitalen Souveränität (Reifegrad) und der Wirkung von Maßnahmen.

BSI, BfDI und der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) erarbeitet und im Rahmen des IT-Rats und IT-Planungsrats abgestimmt, um verbindliche Regelungen zu definieren („Rote Linien der Öffentlichen Verwaltung"). Abhängigkeiten von IT-Anbietern und resultierende Schmerzpunkte sind regelmäßig (max. jährlich) zu analysieren sowie ihre Auswirkung auf die Digitale Souveränität der Öffentlichen Verwaltung zu prüfen. Dies muss nach Möglichkeit für alle Schichten der Technologie-Landschaft iterativ vorgenommen werden. Im Rahmen der Analysen sollen auch Markttrends betrachtet sowie relevante Good-Practices von vergleichbaren Vorhaben aus dem nationalen und internationalen Raum zur Reduzierung von Schmerzpunkten gesammelt werden. Die Ergebnisse hinsichtlich bestehender Abhängigkeiten sowie die Prüfung von Auswirkungen auf die Digitale Souveränität zeigen verschiedene Handlungsoptionen auf und bilden die Grundlage für die strategische Lösungskonzeption.

HF.2: Strategische Lösungskonzeption

Zur Reduzierung von kritischen Schmerzpunkten und Stärkung der Herstellerunabhängigkeit werden gemeinsam mit der jeweiligen Verwaltungsebene Konzepte mit Zielbildern und Maßnahmen erarbeitet und abgestimmt. Dies kann je nach Bedarf sowohl nach Technologie-Schicht oder schichtenübergreifend geschehen. Von herausragender Bedeutung sind dabei Interoperabilität sowie offene Standards und Schnittstellen. Diese Konzepte können auch eine Kombination verschiedener Handlungsoptionen enthalten, z. B. Verhandlung mit aktuellen IT-Anbietern, Mitwirkung an (internationalen) Standardisierungsgremien bzw. -prozessen bis hin zu Aufbau von Alternativen. Bestehende Initiativen (z. B. GAIA-X oder der Europäische Interoperabilitätsrahmen) sollen dabei berücksichtigt werden. Folgend sind die gewählten Optionen zu detaillieren und hinsichtlich ihres Potentials für die kontinuierliche Stärkung der Digitalen Souveränität zu bewerten. Bei der Konzeption von Alternativen wird die technische Machbarkeit iterativ, durch dezentral durchgeführte Proofs of Concepts, bewertet. Die verschiedenen Lösungsansätze werden dabei zentral durch das BMI koordiniert[5]. Darüber hinaus sollen bestehende Alternativen auf Ebene von Bund, Ländern und Kommunen sowie international berücksichtigt werden. Alternativen sollten vorzugsweise, aber nicht zwingend, auf Open Source[6]-Produkten basieren, mindestens jedoch auf offenen Standards und Schnittstellen. Der Aspekt der Digitalen Souveränität und die dazu erforderliche Reduzierung kritischer Schmerzpunkte ist im Rahmen der Wirtschaftlichkeitsuntersuchungen angemessen zu berücksichtigen. Des Weiteren müssen spezifische und allgemeine Anpassungsbedarfe in rechtlichen und organisatorischen Vorgaben, insbesondere in den Bereichen Datenschutz und Beschaffung, identifiziert und notwendige Veränderungen vorbereitet werden.

[5] Die Koordinierung beinhaltet explizit nicht die Beauftragung, Entwicklung oder Umsetzung konkreter Lösungen.

[6] Open Source bezeichnet in diesem Zusammenhang quelloffene und freie Software.

HF.3: Entscheidung und Umsetzungsbegleitung

Entscheidungen hinsichtlich des Einsatzes erarbeiteter machbarer Lösungen und Konzepte sind in individueller Verantwortung der jeweiligen Verwaltungsebene zu treffen. Wo möglich und sinnvoll, streben Bund, Länder und Kommunen eine größtmögliche Konvergenz bei der Entscheidungsfindung und Durchführung von Maßnahmen an, ohne dabei individuelle Vorhaben der anderen Verwaltungsebenen zu behindern. Eine strategische Umsetzungsbegleitung unter Aufsicht der jeweiligen Gremien und Hausleitungen stellt einen Erfolgsfaktor bei der Umsetzung von Maßnahmen dar.

HF.4: Koordination sowie Abstimmung zwischen Bund, Ländern und Kommunen

Informationen und Erfahrungswerte werden zwischen Bund, Ländern und Kommunen ausgetauscht, um ein gemeinsames Verständnis und Transparenz zu schaffen, vor allem hinsichtlich Abhängigkeiten und Schmerzpunkten. Weitere Vorgehensweisen werden soweit möglich und sinnvoll abgestimmt. Sowohl die zu untersuchenden IT-Anbieter, als auch mögliche aufzubauende Alternativen sollen im föderalen Umfeld (Bund, Länder und Kommunen) koordiniert und abgestimmt werden. Durch das gemeinsame Vorgehen wird eine breite Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung angestrebt und es werden Skaleneffekte gehoben. Die Möglichkeit zentraler Beschaffung alternativer Technologien soll sichergestellt werden. Die Abstimmungen erfolgen im Rahmen bestehender Gremien, insbesondere dem IT-Rat/der Ko-ITB, dem IT-Planungsrat und der Arbeitsgruppe „Cloud und Digitale Souveränität“ sowie unter Einbeziehung der FITKO und weiterer relevanter Ansprechpartner[7]. Darüber hinaus soll auf EU-Ebene ein Austausch zu Vorhaben, Ergebnissen und Erkenntnissen stattfinden.

HF.5: Austausch mit Experten

Der Austausch mit Experten auf nationaler und internationaler Ebene wird aktiv verfolgt, um vergleichbare Vorhaben zu analysieren, von deren Erfahrungen zu lernen und eigene Konzepte erfolgreich fortzuentwickeln. Der Fokus liegt neben Deutschland auf dem EU-Raum. Mögliche Experten kommen sowohl aus dem öffentlichen, wissenschaftlichen als auch privaten Bereich und schließen Verbände, Interessensgemeinschaften und Open Source Communities mit ein.

Zusammenfassung und Ausblick

Bund, Länder und Kommunen wollen Maßnahmen entlang der beschriebenen Handlungsfelder zur kontinuierlichen Stärkung der Digitalen Souveränität nach Abgleich mit **bestehenden IT-Zielen**[8] (siehe Anhang A) und unter Berücksichtigung des Datenschutzes, in gemeinsamer Abstimmung planen und umsetzen.

[7] Beispiele für weitere relevante Ansprechpartner sind u. a. die Innenministerkonferenz, die Bundesvereinigung der kommunalen Spitzenverbände, Datenschutzkonferenz sowie die für Vergaberecht zuständigen Bundes- und Landesministerien.

[8] Grundlage sind hier v.a. die IT-Strategie des Bundes (IT-Rat, Beschluss-Nr. 2017/6) sowie die Nationale E-Government Strategie (IT-Planungsrat, Entscheidung 2015/07 bzw. Fortschreibung in Entscheidung 2015/27). Es handelt sich um keine abschließende Liste.

Das vorliegende Eckpunktepapier deckt dabei das weit gefasste Themenfeld „Digitale Souveränität“ nicht vollständig ab. Unter zahlreichen Aspekten obliegt die angemessene und nachhaltige Beantwortung der mit den einzelnen IT-Zielen einhergehenden Fragen weiteren fachlich zuständigen Stellen in den Verwaltungen. Erst die Bündelung der Kompetenz aller dieser Stellen bietet die Gewähr einer umfassenden, angemessen vielschichtigen und lösungsorientierten Betrachtung.

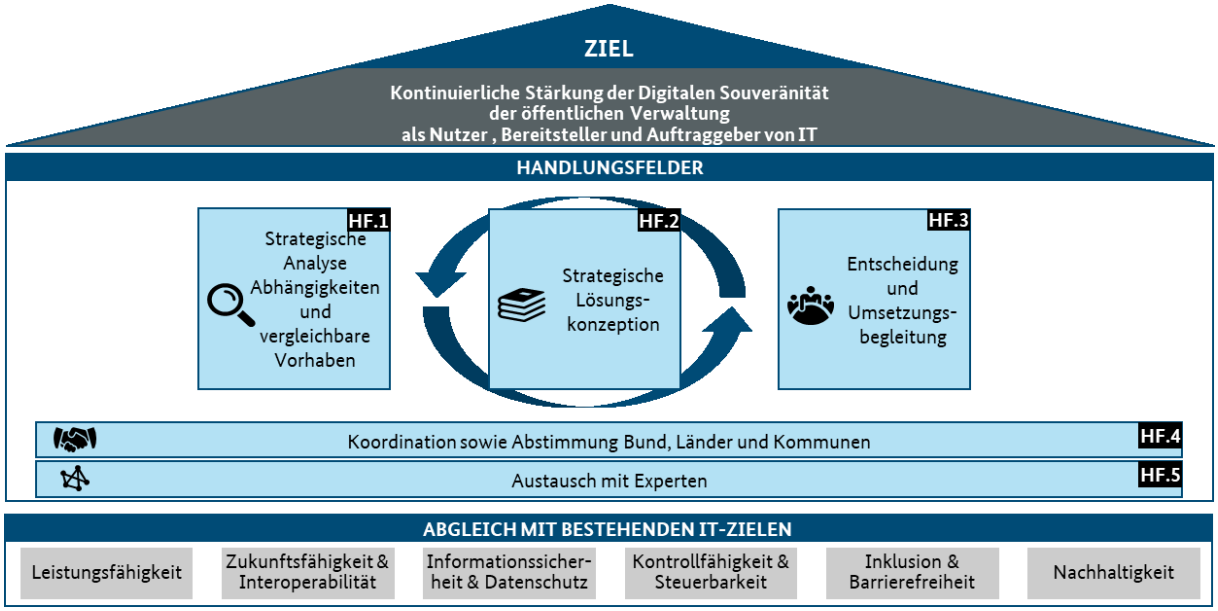

Abbildung 2: Überblick Ziel, Handlungsfelder und Abgleich mit bestehenden IT-Zielen

Das Ziel einer gemeinsamen digitalen – und in diesem Kontext souveränen – Öffentlichen Verwaltung erfordert eine enge Koordination zwischen Bund, Ländern und Kommunen. Die Erreichung dieses Ziels ist eine langfristige und fortlaufende Aufgabe und erfordert eine iterative Annäherung. Maßnahmen sollten in den relevanten Gremien transparent kommuniziert und ggf. koordiniert werden.

Aufgrund der tendenziell steigenden Einschränkung der Digitalen Souveränität der Öffentlichen Verwaltung ist ein schnelles Handeln notwendig. Bei der Umsetzung und für die Zusammenarbeit wird das BMI die übergreifende Koordinierung wahrnehmen.

Anhang A: IT-Ziele (nicht abschließend)

Leistungsfähigkeit

Erarbeitete Maßnahmen sollen die Öffentliche Verwaltung bei der Erfüllung ihrer Aufgaben anforderungs- und bedarfsgerecht unterstützen. Lösungen müssen sich am Nutzen für Bürgerinnen und Bürger sowie für Unternehmen und Verwaltung, inklusive Nutzerfreundlichkeit orientieren. Der stärkeren Professionalisierung der IT zur Erfüllung komplexer werdender Anforderungen ist Rechnung zu tragen.

Zukunftsfähigkeit und Interoperabilität

Der Arbeitsplatz der Zukunft (z. B. orts-, zeit-, und geräteunabhängiger Zugriff) soll vorausschauend gestaltet werden. Interoperabilität (v. a. offene Schnittstellen), Skalierbarkeit, modulare Nutzungsmöglichkeit sowie Übertragbarkeit von Lösungen auf technischer und organisatorischer Ebene müssen so weit möglich sichergestellt werden. Hierdurch soll die eigenständige Innovationsfähigkeit der Öffentlichen Verwaltung langfristig gesichert werden.Zudem sollen Innovation und Veränderungsbereitschaft gestärkt und gefördert und in der Aus- und Fortbildung berücksichtigt werden.

Informationssicherheit und Datenschutz

Die zentralen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit müssen umgesetzt werden. Für die Bundesverwaltung gelten in Bezug auf die Informationssicherheit die Vorgaben des Umsetzungsplan Bund (UP Bund). Rechtliche Rahmenbedingungen wie z. B. die DSGVO sind einzuhalten

Kontrollfähigkeit und Steuerbarkeit

Eine effektive, strukturierte und übergreifende Steuerung der IT soll sichergestellt werden. Aufgaben und Kompetenzen sind klar abzugrenzen und zuzuweisen und klare Regelungen der Auftraggeber und Vertragsverhältnisse sicherzustellen.

Inklusion und Barrierefreiheit

Die Chancengleichheit in der Verwaltung soll gefördert werden durch digitalen Zugang für Menschen mit Behinderung ohne Reduzierung des Funktionsumfangs. Digitale Prozesse wie z. B. digitale Behördengänge, Identifikationsverfahren oder Dokumentenübermittlung sowie die Technologie-Ausstattung sind barrierefrei zu gestalten.

Nachhaltigkeit

Die elektronische Optimierung von Prozessketten hilft den Energiebedarf und den CO2-Ausstoß bei Anbietern und Nachfragern öffentlicher Leistungen zu senken und fördert so die ökologische Nachhaltigkeit. Grundsätzlich sind Verfahren und Technologien einzusetzen, die neben der Leistungsfähigkeit und Wirtschaftlichkeit auch Aspekte der Umweltverträglichkeit und der Nachhaltigkeit berücksichtigen (Green IT).