Steuerungshoheit, Tempo, Ergebnisse

Bausteine und Fahrplan für eine erfolgreiche digitale Transformation der öffentlichen Verwaltung

Themenpapier der Berliner Digitalinitiative

Zur Berliner Digitalinitiative:

Die Berliner Digitalinitiative ist ein Gesprächskreis wesentlicher Systemintegratoren und IT-Partner der Verwaltung zum Zwecke der Förderung der Digitalisierung der Gesellschaft, insbesondere der öffentlichen Verwaltung. Die Initiative führt Informations- und Hintergrundgespräche mit wesentlichen Akteuren und bringt sich an dieser Stelle in den Dialog zur öffentlichen Diskussion zur Verwaltungstransformation ein.

Intro

Die Initiative unterstützt die Absicht der Bundesregierung, die sichere Digitalisierung der Verwaltung voranzutreiben. Sie erkennt die aktuelle Planung zur Konsolidierung und Modernisierung des Bundes im Bereich der Dienst- und Netz- und Dateninfrastruktur als grundsätzlich richtig an. Gleichwohl will die Initiative einen neutralen Impuls zur Entwicklung einer effizienten, wirtschaftlichen und modernen IT-Landschaft geben. Leitmotiv der Initiative ist die Überzeugung, dass eine moderne, innovative und sichere Verwaltung Voraussetzung und Treiber einer erfolgreichen Digitalisierung in Deutschland ist. Dazu müssen die Leistungen der öffentlichen Verwaltung serviceorientiert sowie bürger- und unternehmerfreundlich sein.

Im Hinblick auf eine gesunde und nachhaltige Fertigungstiefe des Staates braucht die Verwaltung ein partnerschaftliches Netzwerk, mit dem sie gemeinsam die Herausforderungen lösen kann. Die ITK-Wirtschaft kann umfangreiche Kompetenzen und langjährige Erfahrung mit der digitalen Transformation in ganz unterschiedlichen Sektoren bereitstellen. Aus diesem Grund unterstützen ITK-Unternehmen den öffentlichen Sektor bei seinem anspruchsvollen und komplexen Transformationsprozess und werden dabei den Ansprüchen an Wirtschaftlichkeit, Sicherheit und Effizienz gerecht.

Neben der Nutzung externer Kompetenzen sollte der Staat grundsätzlich ergebnisorientierter agieren und dabei einige grundlegende Voraussetzungen erfüllen, um Verwaltungsdigitalisierung zu einer Selbstverständlichkeit werden lassen zu können:

- Die Steuerung von Zielsetzungen (Planung bis Umsetzung) sollte viel häufiger über vergleichbare Parameter wie Aufwand, Zeit und Ergebnis erfolgen – nicht Haushaltsmittel, sondern Ergebnisse zählen.
- Interdependenzen müssen verstanden und in den Architekturen sichtbar werden.
- Best Practices helfen, die Komplexität zu reduzieren, und müssen Vorrang haben.
- Anstelle komplexer Eigenentwicklungen sollte der Staat etablierte Lösungen anwenden.
- Eine stringente Governance und ein klares Leitbild sind unerlässlich, damit die Vorteile der Digitalisierung von allen Akteuren verstanden und in die Praxis umgesetzt werden können.
- Transformationsmaßnahmen begründen sich durch ihre Wirksamkeit (Messung und Transparenz mittels KPIs) exAnte/exPost.
- Die Bindung an Benchmarks (z.B. EU-eGovernment Index) ermöglicht das Setzen von Zielmarken.
- Verteilte Zuständigkeiten müssen von den Zuständigkeiten für die operative Ausführung getrennt werden, z.B. sollte ein KFZ-Zulassungsverfahren alle Zuständigkeiten bedienen können.
- Unabhängige Gremien (z.B. der NKR) sollten zur Messung und Bewertung der Qualität staatlichen Handelns mandatiert werden.
- Ergebnisorientierte Arbeitsmethoden müssen im Dienst- und Verwaltungsrecht verankert werden.

- Staat und Verwaltung müssen neue Technologien schnell (möglichst unter sechs Monaten) in den Einsatz bringen können, ebenso sollten das BSI und IT-Sicherheitsgesetz Zertifizierungen zeitnah bereitstellen

Wir konnten beobachten, dass insbesondere der Bund und seine Verwaltung in den letzten Jahren kaum aus dem Krisenmodus herauskommen konnte, weil die Bewältigung der Corona-Pandemie, die weltpolitische Lage und zuletzt der Energieversorgung vielfältige ad hoc Maßnahmen und kurzfristige Anpassungen erfordert haben. Dennoch wurde insbesondere bei der Informationssicherheit und jeweils ressorteigenen IT viel erreicht. Hingegen wurde für eine ressort- oder gar ebenen-übergreifenden Konsolidierung zu wenig erreicht. Das Vorhaben, Bürgerinnen und Bürgern unter Berücksichtigung des Once-Only-Prinzips serviceorientiert Dienstleistungen bereitzustellen, wurde unter der Komplexität zahlreicher anderer Digitalisierungsvorhaben aus den Augen verloren. Dies gilt, obwohl bereits erhebliche Bemühungen wie Ressourcen und nicht zuletzt auch Steuergelder investiert wurden. Unerlässlich für die Erkennung oder Justierung jeglicher staatlich gesetzten Vorhaben ist demzufolge ein Rückblick mit einer ehrlichen Analyse. Auch wenn die Reflexion Zeit in Anspruch nimmt, gewährt sie, dass nachfolgende Projekte und Akteure nicht die gleichen Fehler machen.

Eine erfolgsversprechende Modernisierung der Verwaltung braucht nicht zwangsläufig auf allen Ebenen einheitliche Geschwindigkeit, aber ein gemeinsames Zielbild und ein Betriebskonzept oder Standards, wie dieses Zielbild erreicht werden kann. Dieses zu erstellen ist unsere gemeinsame Aufgabe als Gesellschaft und auch die hier repräsentierten Partner fühlen sich diesem Anspruch verpflichtet. Nur so erreichen wir Fortschritt.

Um in einzelnen Bereichen erfolgreiche Rahmendbedingungen für eine Governance samt Betriebssystem festlegen zu können, empfiehlt die Berliner Digitalinitiative folgende Schwerpunktsetzung für die Verwaltungsdigitalisierung:

1. OZG ist eine Daueraufgabe
2. Digitale Identitäten sind der Zugang zu Verwaltung
3. Registermodernisierung definiert die Grundlage
4. Cybersicherheit stetig weiterentwickeln
5. Souveräne Cloud-Lösungen brauchen strategische Partnerschaften

1. OZG ist eine Daueraufgabe

Das OZG hat als gesetzliche Vorgabe einen Schwung in die Verwaltungsdigitalisierung gebracht, die ihresgleichen in Vorgängerprojekten sucht. Viele Verwaltungen haben das OZG dazu genutzt, um nicht nur die Zugänge für Bürgerinnen und Bürger zu digitalisieren, sondern auch die in der Verwaltung dahinterliegenden Prozesse.

Dennoch haben die im Rahmen des OZGs initiierten Projekte über vier Jahre massive personelle Kapazitäten in den Verwaltungen und der unterstützenden IKT-Wirtschaft gebunden, die allesamt zu Frustration gegenüber den anderen föderalen Partnern geführt haben. In diesem Sinne ist das gesetzliche Vorhaben, Bürgerinnen und Bürgern 575 Dienstleistungen bis Ende 2022 auch digital

anbieten zu können, gescheitert. Die Ursachen für ein Scheitern des OZGs sind vielfältig. Das beginnt bei dem Aufsetzen der Einer-für-Alle-(EfA-)Planung sowie in der Nachnutzung deren Finanzierung. In der jetzigen Konstruktion der FITKO als operative Einheit des IT-Planungsrates fehlen dem Gremium föderale Kompetenzen, um verbindliche Standards setzen zu können. Dies hat in einigen Verwaltungen dazu geführt, dass EfA-Dienste nicht nachgenutzt wurden, sondern eigens nachgebaut wurden. Aus diesem Grund braucht es:

- Ein vorherrschendes Verständnis innerhalb der gesamten Verwaltung, dass das OZG eine Daueraufgabe zur Verwaltungsmodernisierung ist.
- eine gründliche Evaluation, um aus den Fehlern lernen zu können und sie in Folgeprojekten wie der Registermodernisierung vermeiden zu können.
- ein übergeordnetes Ziel, was mit einer OZG-Novelle (OZG 2.0) erreicht werden soll und vordefinierte Zwischenziele.
- Eine Überwindung des ewigen föderalen Kompetenzstreits zwischen den beteiligten Akteuren, wenn es um die Gewährleistung zentraler Dienste, wie iKFZ geht.
- eine Stärkung der FITKO als föderale Instanz mit ausreichendem Budget und Kompetenzen, die eine wirkungsorientierte Steuerung zugunsten einer ganzheitlichen Governance leisten kann.

2. Digitale Identitäten sind der Zugang zu Verwaltung

Digitale Identitäten sind die notwendige Voraussetzung dafür, dass Bürger auch in der digitalen Welt am Wirtschaftsleben teilnehmen und Verwaltungsleistungen in Anspruch nehmen können. Digitale Identitäten müssen einfach in der Anwendung, sicher und datenschutzfreundlich ausgestaltet sein. Insofern unterstützen wir die im Koalitionsvertrag festgeschriebene Priorisierung des Ausbaus eines vertrauenswürdigen, allgemein anwendbaren Identitätsmanagements. Die Schaufensterprojekte des BMWK begrüßen wir ebenso wie eine mögliche Fortführung des Projekts Digitale Identitäten der Bundesregierung.

Die Ausstellung der digitalen Kernidentität sollte eine hoheitliche Aufgabe sein. In Deutschland ist die mittlerweile einfach nutzbare eID-Funktion des Personalausweises etabliert. Allerdings gibt es hierfür noch zu wenige Anwendungsmöglichkeiten. Diese sollten nun sehr zeitnah systematisch in sämtlichen Fachverfahren verankert werden. Daneben sollte die Verwaltung folgende Schwerpunkte priorisieren:

- Die Nutzerfreundlichkeit der eID sollte weiter verbessert werden durch die zügige Einführung der Smart-eID und hierbei eine möglichst große Reichweite gewährleistet werden.
- Die Entwicklung auf EU-Ebene muss mit in den Blick genommen werden. Mit der Novellierung eIDAS-Verordnung möchte die EU-Kommission festschreiben, dass die Mitgliedstaaten den Bürgern und Unternehmen digitale Wallets zur Verfügung stellen, in denen sie ihre nationale digitale Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerschein, Abschlusszeugnisse, Bankkonto usw.) verknüpfen können.

- Bei den in der Verordnung vorgesehen Wallets muss sowohl ein Höchstmaß an Datenschutz- und -sicherheit sowie Vertrauen sichergestellt werden sowie – durch offene Schnittstellen – ein gesunder Wettbewerb gewährleistet werden.

3. Registermodernisierung definiert die Grundlage

Die Registermodernisierung ist eine wichtige Grundlage dafür, dass Verwaltungsleistungen digital angeboten und Verwaltungsprozesse effizienter gestaltet werden können. Insofern muss sie im Dreiklang mit der Weiterentwicklung des OZG und dem Ziel eines vertrauenswürdigen, allgemein anwendbaren Identitätsmanagements gedacht und umgesetzt werden.

Einen hohen Mehrwert stellt es dar, wenn Daten und Nachweise nicht immer wieder erneut für die Erbringung von Verwaltungsleistungen vorgelegt werden müssen. Für eine erfolgreiche Registermodernisierung muss Folgendes berücksichtigt werden:

- Vor dem Hintergrund der Kritik der Datenschutzkonferenz und aus der Zivilgesellschaft an der Nutzung der Steuer-ID als registerübergreifende Identifikationsnummer sollte unter Akzeptanzgesichtspunkten erwogen werden, für den weiteren Ausbau der Registermodernisierung Technologien in den Blick zu nehmen, die bereichsspezifische Identifizierung nutzen und damit das Risiko von Profilbildung noch weiter minimieren.
- Es braucht einen klaren zeitlichen Rahmen und ein koordinierendes PMO, welches die Interessen der Akteure zugunsten eines ganzheitlichen Zielbildes priorisiert.
- Neben der Nutzerfreundlichkeit muss aber auch ein möglichst hohes Maß an Vertrauen bei den Bürgerinnen und Bürgern gewährleistet sein. Das Datenschutzcockpit, das einen Überblick bietet, welche Behörde auf ihre Daten zugegriffen ist hierfür ein wichtiges Instrument.

4. Cybersicherheit stetig weiterentwickeln

Das BSI beschreibt die Informationssicherheit als Prozess und liefert mit dem Grundschutz-Kompendium eine exzellente fachliche Grundlage für die Absicherung von IT-Systemen in der Verwaltung – und darüber hinaus. Angesichts der zuletzt massiven Angriffe auf IT-Systeme, auch im behördlichen Umfeld, sind wir jedoch auch zu der Überzeugung gelangt, dass es dringend geboten ist, mit der IT-Sicherheit vor die Lage zu kommen: mit Zero-Trust-Architekturen.

Zunächst geht es weniger um einen technischen, sondern organisatorischen Ansatz. Alle IT-Dienste werden einzeln und verursacherunabhängig geprüft. Das kann bis runter zum einzelnen Prozess innerhalb der Fachaufgabe umgesetzt werden. Dieser Services-Ansatz mach „Zero-Trust“ erst möglich. Der Zugriff des Prozesses auf Daten und Informationen wird erst nach einer erfolgreichen Identifizierung und Authentifizierung autorisiert. Daneben gilt:

- Die Verwaltung sollte noch stärker die Erfahrungen der geheimschutzbetrauten Spezialisten in Deutschland nutzen. Viele versammeln sich unter dem Label „IT Security made in Germany“ von TeleTrusT.
- Es kommt darauf an, IT-Sicherheit stetig weiterzuentwickeln und die vorhandenen Lösungen möglichst effizient zum Einsatz zu bringen.
- Ein stetiges Schwachstellenmanagement (insbesondere für „Spezial- und Legacy-Anwendungen“) ist essenziell.
- Für alle laufende Systeme und Plattformen ist regelmäßiges Penetration-Testing unerlässlich.
- Standards „Made in Europe“ stehen unter dem Einfluss von Wechselwirkungen aus digitaler Souveränität und Resilienz. Kleinstaaterei und daraus resultierende Insellösungen müssen vermieden werden. Nur durch ein vernetztes Europa mit geteilten europäischen Werten kann die digitale Souveränität einzelner Staaten gewährleistet werden.
- Cybersicherheit in der Verwaltung ist nicht nur ein Thema der Inneren sondern auch äußeren Sicherheit. Damit die Verwaltungsdigitalisierung in Deutschland gelingt: resilient, souverän, sicher.

5. Souveräne Cloud-Lösungen brauchen strategische Partnerschaften

Die Anforderungen des Bürgers an eine moderne Verwaltung entsprechen denen, die er aus dem privaten Geschäftsverkehr kennt: ein einheitliches Nutzerkonto für alle Verwaltungsvorgänge, Medienbruchfreiheit sowie rund um die Uhr Erreichbarkeit mit einem sehr hohen Grad an Automation. Dies lässt sich nur mit Cloud-basierten Lösungen sicherstellen. Die Umsetzung folgender Punkte ist daher wichtig:

- Differenzierung und Standardisierung: Im Kontext digitaler Souveränität werden verschiedenen technische Anforderungen an Cloud-Lösungen diskutiert. Es braucht keine Eine-für-Alles-Lösung, vielmehr sollte eine Abstufung und Differenzierung je nach je nach Anwendungsfall unter Berücksichtigung geltenden Standards erfolgen.
- Eine verbindliche Festlegung auf Schutzbedarfskategorien würde durch die damit einhergehende Standardisierung für beide Seiten, Kunden wie Anbieter, Vorteile schaffen: So müssen einmal erfolgte Schutzbedarfsprüfungen nicht in Gänze wiederholt werden. Ideal wäre somit eine Gruppe von Schutzbedarfskategorien, anhand derer der Kunde je nach gefordertem Schutzniveau beschaffen kann. Für IT-Lösungsanbieter wird ein Anreiz geschaffen, verstärkt ein eine Lösung zu investieren, da diese einer Vielzahl von Behörden zur Verfügung gestellt werden kann. Spiegelbildlich senkt diese die Kosten für den Auftraggeber.
- Wir brauchen mehr strategische Partnerschaften zwischen IT-Anbietern und öffentlicher Hand. Zwar gibt das Vergaberecht dazu Spielräume, diese werden jedoch zu wenig genutzt bzw. sind zu wenig bekannt. Zudem bestehen auf Kundenseite regelmäßig Bedenken gegen solche Partnerschaften. Daher sollten rechtssichere Modelle für strategischen Partnerschaften erarbeitet und sodann gelebt werden. Die Vorteile solcher Partnerschaften für die öffentliche Hand sind:

- Schnelligkeit: Durch den gegenseitigen Wissenstransfer erreicht die Lösung wesentlich schneller den erforderlichen Reifegrad.
- Praxistauglichkeit: Die Anforderungen der öffentlichen Hand können besser in die Lösung einfließen.
- Innovationsförderung: Für noch-nicht-am-Markt verfügbare Lösungen kann der Anbieter unter definierten und damit für ihn kalkulierbaren Risiken entwickeln.
- Investitionsmöglichkeiten: Die öffentliche Hand hat die Möglichkeit, sich selbst an einem solchen Joint Venture als Gesellschafter zu beteiligen.

Abschluss

Unter Berücksichtigung der oben genannten Schwerpunkte wird es gelingen, die Verwaltungsdigitalisierung in Deutschland unter Steuerungshoheit mit mehr Tempo und erfolgreichen Ergebnissen voranzutreiben. Sie bilden den Baustein und legen einen Fahrplan für eine erfolgreiche digitale Transformation dar.

Wir bedanken uns bei allen Mitgliedern der Berliner Digitalinitiative, die die Erstellung dieses Papiers unterstützt haben.