Themen/Positionspapier der Berliner Digital Initiative 2019

I. Digitalisierung der Verwaltung - Durchgängigkeit des föderalen Systems

Sachstand

Reformerfolge anderer Staaten zeigen, dass eine digitale Verwaltung nur gemeinsam gelingen kann. Durchgängige digitale Angebote setzen eine gemeinsame strategische Gesamtausrichtung, einheitliche IT-Infrastrukturen und einen modernisierten Rechtsrahmen voraus. Dies stellt die Verwaltung in Deutschland mit ihrem föderalen Mehrebenensystem vor große Herausforderungen. Damit diese bewältigt werden können, sind Veränderungen auf allen Ebenen erforderlich – rechtlich, strukturell, technisch und personell – und zu Beginn der nächsten Dekade umzusetzen.

II. Digital first! Kanzleramt als Vorreiter?

Laut dem Digital Economy and Society Index (DESI) aus dem Jahre 2019, mithilfe dessen ein E-Government-Ranking der EU erstellt wurde, befindet sich Deutschland bei der Digitalisierung von Verwaltungsleistungen unter dem EU-Durchschnitt auf Platz 26.

Position der Berliner Digital Initiative

Die Entwicklung des E-Government in Deutschland ist im Vergleich zum EU-Durchschnitt des Digital Economy and Society Index (DESI) beim Ranking negativ. Deutschland erreicht noch Platz 26. Der Normenkontrollrat beschreibt in seinem Monitor Digitale Verwaltung #3 fundamentale Fehler bei der Vorgehensweise. Die Berliner Digitalinitiative sieht keine Chance, das OZG-Ziel 575/2022 zu erreichen. Es fehlen grundsätzliche Entscheidungen zur Authentifizierung, Zentralisierung von Funktionen, einheitliche Standards sowie eine Plattform bzw. eine harmonisierte Plattformlandschaft. Die Entscheidungsstrukturen aus der Steuerungsperspektive Zeit und Effektivität sind ungeeignet.

- Damit der Portalverbund gelingen kann, ist die Entwicklung einer föderalen und auf offene Schnittstellen und internationalen Standards basierende IT-Architektur bei Konsolidierung und Standardisierung ein wesentlicher Erfolgsfaktor → Plattformgedanke für Prozesse, Zuständigkeiten und Prozesse
- Es sollte Teil des Gesamtvorhabens sein, unter Einbeziehung des Nationalen Normenkontrollrats (NKR) zu untersuchen, welche Wesen und Verfahren zukünftig ganz wegfallen könnten.

- Die arbeitsteilige OZG-Umsetzung von Bund, Ländern und Kommunen wird nur zur Entwicklung von Prozessen führen. Was jedoch für den Erfolg der OZG-Umsetzung benötigt wird, sind Fachverfahren: Den Kommunen sollten Plattformen samt Fachverfahren zur Verfügung gestellt werden.

Die für den Portalverbund zu verwendende Technik sowie die Interoperabilitäts- und Sicherheitsstandards kann der Bund als Rechtsverordnung festlegen. Mit § 4 OZG hat der Bund ein großes Fenster geöffnet, um eine weitgehende Standardisierung von Fachverfahren durchzusetzen. Damit der Portalverbund gelingt, ist die Entwicklung einer föderalen IT-Architektur mit gesamtstaatlich verbindlichen Vereinbarungen ein wesentlicher Erfolgsfaktor.

III. Digitale Infrastruktur – Breitband und Rechenzentren

Sichere Rechenzentren, eine sichere Kommunikation- und Kommunikationsinfrastruktur sowie flächendeckende Gigabit-Netze sind das Rückgrat einer modernen digitalen Wirtschaft und Verwaltung. Sie sind Kernbestandteil einer digitalen Infrastruktur, ohne die weder digitale Kommunikation noch andere digitale Dienste funktionieren können. Sie sind Ausgangspunkt und Basis für Wettbewerbsfähigkeit, technologischen Fortschritt, Datensicherheit und digitaler Versorgung/Vorsorge. Die Festlegung verbindlicher Sicherheitsstandards ist eine Grundvoraussetzung zur Erhöhung der Informationssicherheit.

Nur Gigabit-Netze können die Anforderungen an eine leistungsfähige digitale Infrastruktur erfüllen, und sollten zukünftig als Synonym für moderne Netze verwendet werden. Der Begriff „Breitband“ ist ungeeignet, da er keine Mindestgeschwindigkeit beschreibt und in der Vergangenheit schon für Bandbreiten ab 1 Mbit/s benutzt wurde.

These 1: Deutschland hat (im Verhältnis zu vergleichbaren Industrieländern) einen erheblichen Rückstand im Ausbau von Gigabit-Netzen. Das gilt es anzuerkennen und mit geeigneten regulatorischen Maßnahmen zu beheben. Die meisten Geschäftsmodelle der digitalisierten Wirtschaft sind essentiell abhängig von der Verfügbarkeit hoher Bandbreiten (ab 1 Gbit/s)

These 2: Rechenzenten bilden (gemeinsam mit Gigabit-Netzen) das Fundament der digitalen Wirtschaft eines Landes. Fast die gesamte digitale Wertschöpfung findet letztendlich in Rechenzentren statt. Die Server, Speichersysteme und Netzwerkkomponenten in den Rechenzentren ermöglichen erst die vielfältigen digitalen Services, die heute und in Zukunft genutzt werden. Deutschland ist (insbesondere aufgrund des hohen Strompreises und der EEG-Umlage) der teuerste Standort für Rechenzentren in Europa. Trotz deutlichen Wachstums entwickelt sich der Rechenzentrumsmarkt unterproportional. Wenn die Rahmenbedingungen für Rechenzentren nicht angepasst werden, kommt es zur weiteren Abwanderung von IT-Systemen (und den damit verbundenen Kompetenzen, Arbeitsplätzen und Umsätzen) hauptsächlich nach Frankreich, den Niederlanden und Skandinavien oder in außereuropäische Länder. Das widerspricht dem Gedanken einer konzertierten Aktion zur Umsetzung von GAIA-X.

IV. IT-Konsolidierung des Bundes

Die Diskussion um die IT-Konsolidierung des Bundes wurde vor 10 Jahren über eine Initiative des Haushaltsausschusses des Deutschen Bundestages angeregt. Ein Bericht des Bundesinnenministeriums zeigte seinerzeit die desolate Lage der Gesamtsituation: mehrere hundert Rechenzentren bzw. Serverräume, keine Standardisierung und damit auch mangelnde Sicherheitsvoraussetzungen. Getrieben durch den Haushaltsausschuss des Bundestages hat sich dann die Bundesregierung unter Federführung des Bundesinnenministeriums (BMI) auf den Weg gemacht eine Diskussion über die Konsolidierung des Bundes im Bereich der Rechenzentren und der Fachverfahren auf den Weg zu bringen. Federführend waren zeitweise das Bundesinnenministerium, hier Herr Staatssekretär Vitt, das Bundesfinanzministerium, hier Herr Staatssekretär Gatzer (derzeit) und das Bundesverteidigungsministerium (früher Staatssekretärin Suder, heute Staatssekretär Zimmer). Nachdem diese Diskussionsprozesse weitestgehend in Differenzen ausgetragen wurden, liegt nun eine neue Kostenschätzung für das Gesamtvorhaben vor. Statt von knapp unter einer Milliarde Euro soll das Gesamtvorhaben 3,5 Milliarden Euro ausmachen. Dazu gehören die Ertüchtigung der einzelnen Ressorts für den Übergang in eine zentrale IT, die Ertüchtigung vor allem der BWI als Tochter der Bundeswehr für die Übernahme von Kunden aus dem Kreis der Bundesressorts und den weiteren Ausbau des ITZBund, früher Zivit (Rechenzentrum des Bundesfinanzministeriums). Die Bemühungen getrieben durch den Haushaltsausschuss blieben dann aber stecken, auch wegen der Kostenexplosion. Das Bundeskanzleramt hat sich nun moderierend in den Prozess eingeschaltet und in einer einvernehmlichen Regelung wurde festgehalten, dass das BMI für die Konsolidierung der Dienste und das BMF für die Konsolidierung des Betriebes zuständig sein sollen. Gleichzeitig wurde festgelegt, dass die BWI (Bundeswehr) nur noch als Unterauftragnehmer des ITZBund (BMF) tätig werden soll.

Daraus ergeben sich aktuell Probleme, weil einige der BWI- Kunden nun rückabwickeln müssen. Das bedeutet für die betreffenden Ressorts Reinvestition in die hauseigene IT. Im Haushalt für das nächste Jahr gar nicht vorgesehen und schon gar nicht das Personal. Generell sollen sie vom ITZBund betreut bzw. übernommen werden, müssen aber wegen der beschränkten Kapazitäten mit einer zeitlich nach hinten versetzten Übernahme rechnen, also einer Einordnung in die Priorisierungsliste des ITZBund.

Die zersplitterte und föderale Struktur einheitlich möglicher Informationstechnologien wird dabei sowohl weiterhin durch Ressort- wie auch Ländergrenzen blockiert.

Die Rückabwicklung der IT einiger BWI-Kunden führt nun zu einem Neuaufbau in technologischer, infrastruktureller, personeller und Lizenzsicht einzelner Ministerien. Damit dürfte der IT-Konsolidierung ein Verlängerungsschub von etlichen Jahren folgen.

Das ITZBund hat bekanntgegeben, dass eine neue Priorisierung der Abfolge der Integration einzelner Ressorts in den IT-Konsolidierungsprozess damit notwendig werden würde. Realistisch betrachtet bedeutet das, dass die IT-Konsolidierung des Bundes um mindestens fünf

Jahre in ihrer Gesamtheit sich verzögert. Zudem kommt, dass das ITZBund wegen seiner neuen Ausschließlichkeit als zentrale IT-Dienstleister deutlich mehr Personal benötigt.

Daraus ergeben sich Fragen, die die Bundesregierung noch nicht beantwortet hat:

- Wie soll das ITZBund personell und strategisch ausgestattet werden, um seine Aufgabe als einziger zentraler Dienstleister der IT-Konsolidierung gerecht werden zu können?

- Das ITZBund wird als Anstalt des öffentlichen Rechts ausgestattet. Mit einer relativen Eigenkompetenz und einem Aufsichtsrat oder weiterhin als eine Anstalt des öffentlichen Rechts, die dem Bundesfinanzministerium in direkter Weise untersteht ist noch unklar. Wäre es an dieser Stelle nicht sinnvoll dem letztlich erfolgreichen Modell des Verteidigungsministeriums zu folgen und eine ÖPP zu organisieren, die in Sachen konsequenter Standarisierung, Einsatz des Personals in gemischter Form aus öffentlichen und privaten Ressourcen sowie einer vertraglichen Grundlage über die Leistungserbringung zwischen privat und öffentlich in der Lage wäre in einem gesetzten Zeitrahmen die Umsetzung der Konsolidierung zu gewährleisten?

  Im Verteidigungsministerium wurde bereits eine Diskussion darüber geführt, ob nicht ein Herkules II sinnvoll für die Realisierung dieses Vorhabens, der IT-Konsolidierung des Bundes sei. Betrachtet man alle Vor- und Nachteile des Herkules-Prozesses, aus dem sich die mittlerweile erfolgreich tätige BWI ergeben hat, ergibt sich durchaus zwingend die Überlegung, dass eine öffentlich-private Kooperationsgemeinschaft zur Erreichung der Ziele der IT-Konsolidierung als durchaus sinnvoll erscheint. Nicht nur vor dem Hintergrund, dass die Diskussion über zehn Jahre läuft und ohne Erfolg bisher verblieben ist, sondern auch aufgrund der Tatsache, dass eine Kostenkontrolle derzeit nicht gegeben ist. Diese könnte durch eine vertragliche Vereinbarung zwischen öffentlich und privaten Investoren in eine ÖPP-Gesellschaft eindeutig geregelt und damit auch gedeckelt werden. Trotz aller schmerzhaften Prozesse der Bundeswehr bei der Realisierung des Herkules-Vorhabens, das zum erfolgreichen Abschluss der BWI führte, die mittlerweile wieder zurück in den Besitz des Bundes gegangen ist, scheint dies eine sinnvolle Perspektive zu sein.

  Zudem wurde bisher in unausreichendem Maße das Thema IT- und Cyber- Sicherheit bei dem gesamten Projekt vernachlässigt. Der Bundesrechnungshof (BRH) hat dies in einer Stellungnahme dezidiert dargelegt und der Haushaltsausschuss des deutschen Bundetags aufgegriffen und auch hierzu ein Konzept vor Freigabe der Finanzmittel von der Bundesregierung verlangt.

These 1: Der Bund wird nicht in der Lage sein in den nächsten Jahren aufgrund der eingetretenen Rückabwicklung von Einzelkunden der BWI zurück in die eigenen Ressorts der Bundesministerien zu einer konsequenten und stringenten Linie in der Umsetzung des IT-Konsolidierungsverfahrens zu kommen.

These 2: Eine Kostendeckelung ist bei Betrieben und öffentlichen Unternehmen ohne vertragliche Grundlage erfahrungsgemäß nicht zu kontrollieren und damit sind “unkontrollierte“ weitere Budgetaufstockungen unausweichlich.
These 3: Nur eine konsequente Umsetzung von Standarisierung, Vereinheitlichung und Zusammenführung – und somit auch Reduzierung der Eigenwege der Ressorts in Sachen IT – ist durch eine zentrale marktwirtschaftlich orientierte ÖPP zu erreichen.
These 4: Bei Bildung einer neuen Bundesregierung wird es zur Neuressortierung kommen. Die Diskussion muss bereits jetzt darüber geführt werden welche Verantwortlichkeiten ein Digitalisierungsministerium hat- besonders mit Blick auf das Gesamtbudget-, welche Rolle weiterhin das BMI (strategisch, konzeptionell mit Blick auf die Verwaltung selbst), das BMF mit Blick auf den Betrieb und das Bundeskanzleramt mit Blick auf die strategische Koordination des Gesamtprozesses behalten werden.

V. Digitalstrategie der Bundesregierung – Umsetzungsstrategie zur Gestaltung des Digitalen Wandels

Die im November 2018 vom Kabinett beschlossene Umsetzungsstrategie fasst 111 Maßnahmen in fünf Handlungsfeldern zusammen und beschreibt deren Zielsetzung, Finanzierung und Zeitplan.

Position der Berliner Digital Initiative

Die Berliner Digital Initiative begrüßt die Umsetzungsstrategie zur Gestaltung des Digitalen Wandels. Insbesondere vor dem Hintergrund des internationalen Wettbewerbs von KI und weiteren digitalen Geschäftsmodellen, ist es wichtig, dass Deutschland so schnell wie möglich Standards setzt und wettbewerbsfähig wird.

Jedoch ist anzumerken, dass es der Digitalstrategie an einem konsistenten und strategischen Ansatz mangelt. Zu begrüßen wären grundlegende Entscheidungen hinsichtlich der Ziele, wie sich Deutschland im Rahmen des digitalen Wandels international positionieren will. Die Probleme werden in der Strategie ausführlich analysiert, doch es fehlen bisweilen die Lösungen: Welche Rolle soll Deutschland bei der Abbildung gesellschaftlicher und rechtlicher Normen in technische Realitäten einnehmen und welche Standards muss der Staat selbst bei eigenen Projekten erfüllen? Diese strategischen Fragen stehen aktuell im Raum und benötigen eine schnelle Klärung, damit die Chancen von KI und Big Data verantwortungsvoll realisiert werden können. Auch mangelt es an konkreten Daten für die meisten Projekte sowie an konkreten Budgets. Ebenso eine Priorisierung der Projekte und Indikatoren für die Zielerreichung fehlen. Es sollte überlegt werden, wie die Regierung die technologische und marktbezogene Wettbewerbssituation Deutschlands befördern kann. Modelle der JV Finanzierung wie in den USA und Israel erfolgreich praktiziert sind unbedingt zu adaptieren und die notwendigen Mittel bereit zu stellen.

VI. IT-/Cyber Security

IT-/Cyber Security muss einerseits die ständig wachsenden externen Bedrohungsszenarien bewältigen, sich andererseits im Kontext der digitalen Transformation von Staat und Gesellschaft weiterentwickeln. Mit der wachsenden Bedeutung von auf Daten basierenden Geschäftsmodellen und -prozessen wird sich Cyber Security immer mehr zu einer Schlüsseltechnologie entwickeln. Ein Identitäts- und Rechtemanagement ist dabei eine der Voraussetzungen für die sichere, transparente und effiziente Bereitstellung von zentralen Diensten in einer verteilten und heterogenen IT-Infrastruktur.

Verteilte Kompetenzen im Bereich Cyber Security

In der jüngeren Vergangenheit wurden durch verschiedene gesetzliche Regelungen die Kompetenzen im Bereich Cyber Security neu strukturiert und zum Teil erweitert. Gleichzeitig wurden kritische Infrastrukturen unter eine engere Kontrolle gestellt.

These 1: In Deutschland gibt es vielfältig aufgeteilte Verantwortlichkeiten und Kompetenzen im Bereich Cyber Security.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) koordiniert mit dem Nationalem Cyber-Abwehrzentrum (Cyber-AZ) die verschiedenen Informationen von BfV, MAD und BND aus nachrichtendienstlicher Sicht, BKA, ZKA und BPOL aus polizeilicher Sicht und das BBK schließlich aus Sicht der Katastrophenvorsorge und der kritischen Infrastrukturen. Die Fähigkeiten und Kompetenzen verbleiben aber bei den ursprünglichen Behörden. Darüber hinaus gibt es noch weitere Stellen, die Kompetenzen im Bereich der Cyber Security wahrnehmen. Neben der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) im Bereich BMI, der Agentur für Innovation in der Cybersicherheit im Bereich von BMVg und BMI ist auch das Cyber Innovation Hub im Bereich des BMVg zu nennen. Zusätzlich sind auch auf Länder- und Kommunalebene weitere Kompetenzen vorhanden.

These 2: Die Einbettung in verschiedene Ressorts schafft keine vollkommene Unabhängigkeit und Handlungsfähigkeit im Bereich Cyber Security.

Die Zuordnung zu verschiedenen Ressorts und durch die föderalistische Staatsorganisation sind verschiedenste Verantwortlichkeiten und Kompetenzen entstanden, die nur schwerlich das Thema Cyber Security umfänglich abdecken können. Neben der Spezialisierung auf bestimmte Bereiche fehlt jedoch eine ganzheitliche strukturelle Bündelung der Kompetenzen, also eine Ausgestaltung der Ziele der Cyber-Sicherheitsstrategie.

Position der Berliner Digital Initiative

> Die Kompetenzen im Bereich Cyber Security müssen besser gebündelt werden, um ein gesamtstaatlich angemessenes Sicherheitsniveau zu erreichen!
>
> Ebenso muss es ein politisches Ziel der Bundesregierung sein, die Kompetenzen im Bereich Cyber Security unabhängiger von einzelnen Ressorts zu machen.

VII. Digitale Identitäten, Vertrauensdienste und Identity Access Management (IAM)

Im Kontext der digitalen Transformation entstehen immer mehr digitale Identitäten und das sichere Management von Identitäten und Daten wird zunehmend zu einem Gradmesser für die Innovationsfähigkeit von Wirtschaft, Staat und Verwaltung. Dabei weichen analoge Sicherheitsmerkmale und Prüfungen zunehmend einer digitalen Identifizierung, Verschlüsselung und Signatur sowie deren Verifikation. Neue Konzepte und Entwicklungsprojekte stellen den Bürger bzw. den Nutzer in den Fokus und machen ihn zum Herr seiner Daten. So ermöglicht beispielsweise das Konzept der Self-Sovereign-Identity (SSI) ein Single-Sign-On System zur Verwaltung unterschiedlicher Konten. Dabei wird ein Datentresor auf einem Mobiltelefon eingerichtet und verschiedene Anbieter können dafür Apps anbieten. Die Verwaltung der digitalen Identität liegt somit nicht bei einer zentralen Instanz, sondern beim Nutzer selbst. Nachdem eine Behörde die hinterlegten Daten einmal verifiziert hat, kann die digitale Identität für behördliche Leistungen, wie zur digitalen Signatur der Steuererklärung oder zum Nutzen privater Dienste, wie dem Onlinebanking, genutzt werden.

Auch das Förderprojekt OPTIMOS ist ein wichtiger Schritt hin zu nutzerfreundlichen digitalen Identitäten. Dabei wird ein offenes, praxistaugliches Ökosystem geschaffen, bei dem wesentliche Daten im Secure Element eines Handys gespeichert werden. So kann der Personalauweis beispielsweise auf das Handy übertragen (abgeleitet) werden. Mithilfe dieser Technologie werden eID-Diensteanbieter in die Lage versetzt, mobile eID-Services mit hohem oder substanziellem Schutzniveau anzubieten. Dies ist insbesondere für Dienstleistungen wie Carsharing oder Onlinebanking von Bedeutung, die ein hohes Sicherheitsniveau voraussetzen.

Position der Berliner Digital Initiative
Eigene europäische Standards unter Berücksichtigung neuester technologischer Ansätze sind Voraussetzung für die digitale Souveränität Europas im Bereich der digitalen Identitäten und Vertrauensdienste. Sie sind Grundvoraussetzung für digitale Dienstleistungen der Verwaltung. Gleichzeitig ist eine leicht zu nutzende staatliche/staatlich beauftragte ID mit differenzierten Vertrauensniveaus auch für Mittelständler und Start-Ups wichtig, weil sie Voraussetzung für sichere und skalierbare Transaktionen im Netz ist und gleichzeitig die Abhängigkeit von großen global agierenden Digitalkonzernen reduziert, die digitale Identitäten von Endnutzern heute größtenteils kontrollieren. Dasselbe gilt für Inhaber digitaler Identitäten, die bei der Nutzung einer staatlichen digitalen ID keinen Datenabfluss befürchten müssen. Gleichzeitig ist für Endnutzer eine hohe Zahl von Use Cases sowohl gegenüber der Verwaltung als auch gegenüber dem Privatsektor ein wichtiger Anreiz zur Nutzung digitaler Identitäten.

Auf EU-Ebene ist die eIDAS-Verordnung der wichtigste europäische Standard für digitale Identitäten und Vertrauensdienste. Sie definiert die Anforderungen für die Zertifizierung und EU-weite Anerkennung dieser Dienste. Der Verordnung fehlt es aber bisher an Verbindlichkeit was die Nutzung und Akzeptanz der Dienste betrifft. Dies gilt etwa für Anbieter von Browsern, welche mittlerweile in der Lage sind, eigene Standards zu setzen und europäische Marktteilnehmer aus dem Markt zu drängen. Nach eIDAS zertifizierte Websitezertifikate werden

bislang von den Browsern nicht anerkannt, sondern müssen zusätzliche von den Browserherstellern definierte Anforderungen erfüllen. Hier bedarf es einer europäischen Antwort, die konsequent auf einen europäischen Vertrauensraum setzt und die Akzeptanz von eIDAS-Diensten durch Global Player für die EU verbindlich vorschreibt. Schon seit 2014 ist die eIDAS-Verordnung in Kraft und ermöglicht (zumindest in der Theorie) sichere und einfache digitale Verwaltungs- und Geschäftsprozesse in der Europäischen Union. Die eIDAS-Vertrauensdienste wie das qualifizierte elektronische Siegel wurden allerdings noch nicht überzeugend in das deutsche Recht integriert und entfalten daher bislang keine große Wirkung. Mithilfe qualifizierter Website-Zertifikate können etwa Webseiten von Krankenhäusern, Behörden oder Banken abgesichert werden. Für eine flächendeckende Anwendung müsste der Einsatz qualifizierter Website-Zertifikate im Telemediengesetz festgeschrieben werden. Ein gutes Beispiel für die rechtliche Verankerung der Vertrauensdienste ist die Zahlungsrichtlinie PSD2 (Payment Services Directive 2). Dort sind die Werkzeuge der eIDAS-Verordnung zur Absicherung der Kommunikation zwischen Banken und Drittanbietern rechtlich vorgeschrieben. Die Richtlinie könnte Vorbild für eine ähnliche Umsetzung in anderen Anwendungsfeldern sein. Zudem bietet es sich an zusätzlich zu dem Projekt „Bessere Rechtssetzung“ des Bundesministeriums des Innern, für Bau und Heimat, eine Folgenabschätzung durchzuführen, welche überprüft, ob ein Gesetz digitalisierungsfreundlich ist. Einer der zu überprüfenden Punkte wäre, inwiefern Vertrauensdienste im Gesetzestext berücksichtigt wurden und ob sie jetzt auch tatsächlich Anwendung finden. Auf diese Weise würde man die eIDAS-Vertrauensdienste als wichtiges Mittel digitalisierungsfreundlicher Gesetzgebung anerkennen. Außerdem bietet die deutsche EU-Ratspräsidentschaft im kommenden Jahr die Chance, die Weiterentwicklung der eIDAS-Verordnung auf die Agenda des Europäischen Rats zu setzen. So könnten die Vertrauensdienste etwa um eine eID-Funktion für Unternehmen erweitert werden, um eine Anwendung entsprechend für juristische Personen zu generieren.

VIII. Innovation und Innovative Technologien

Die Berliner Digital Initiative setzt sich für die Schaffung von Innovationen durch die Etablierung eines kreativen Umfeldes sowie der Einsatz innovativer Technologien in der Öffentlichen Verwaltung ein. Sie fordert die Schaffung von Innovationszentren (Innovation Hubs), in denen IT-Unternehmen, Start-ups, Forschungsinstitute und staatliche Institutionen fallbezogen kooperieren, um neue Dienste auf Basis innovativer Technologien (Blockchain, Künstliche Intelligenz, ChatBots, Big Data Analytics etc.) zu entwickeln.

Robotics &Automation

Automation und Robotics werden zum neuen Trend im Zuge der Digitalisierung. Die neuen Technologien ermöglichen die Automatisierung von Routinetätigkeiten, Informations- und Auskunftsdienste, Auswertungen, Eliminierung manueller Datenübertragungen zwischen verschiedenen Systemen oder die intelligente und agile Orchestrierung von einzelnen Verfahren und prozessschritten zu ganzheitlichen Lösungen und können damit eine effektive Antwort auf das Problem des Demografischen Wandels sein.

Cloud Computing

Mit dem Trusted Cloud Label, das im Markt positiv aufgenommen wurde und sich etabliert hat, und NExT dem ressortübergreifenden Netzwerk aus Vordenkenden und aktiv Gestaltenden der Digitalisierung im öffentlichen Sektor sind bereits gute Initiativen vorhanden. Somit sind einige Rahmenbedingungen und erste Richtlinien geschaffen. Mit der Einführung der Bundes-Cloud wurde ein wichtiger Schritt getan. Ein Cloud First Ansatz ist zu erkennen. In vielen Bereichen geht es voran, allerdings nicht überall. Es fehlt vor allem an der tatsächlichen Umsetzung einer ganzheitlichen Strategie der Vision zum Thema Cloud. Mögliche Ansätze wäre ein Resort übergreifendes Transformationsprojekt welches die verschiedenen Ebenen der Politik Länder, Behörden und Kommunen zusammenführt aber dabei der IT mehr Entscheidungskraft gibt.

Gerade für Kommunen, die unter Kostendruck leiden, kann die Public Cloud mit ihren kostengünstigen, schnellen Lösungen mit Augenmaß und die entsprechenden sicherheitsrelevanten Aspekte betrachtet, gute Lösungen bieten. Der Multi-Cloud Ansatz mit dem Besten aus der Public- bzw. Private-Cloud gilt in der Industrie schon so gut wie gesetzt.

Die Verwaltung im öffentlichen Dienst mit Ihren vielen Ebenen steht vor besonderen Herausforderungen. Evtl. ist mit der Transformation der Behörden im Rahmen der Cloud ein komplettes Umdenken der Strukturen notwendig damit man zukünftig erfolgreich sein kann. Siehe Einführung der X-Road in Estland.

Blockchain

Die öffentliche Verwaltung regelt das gesellschaftliche Zusammenleben und ist Vermittler zwischen Bürger und Staat. Dabei stellt die Verwaltung Register zur Verfügung, denen ein öffentliches Vertrauen zukommt und ist für die Beglaubigung der Echtheit von Unterschriften unter Dokumenten verantwortlich. Im digitalen Zeitalter ist die Blockchain das erwähnte Register. Die Blockchain ermöglicht die lückenlose sichere Nachvollziehbarkeit, Unangreifbarkeit und Integrität. Smart Contracts, Bestandteil der Blockchain, ermöglichen die Automatisierung von Verwaltungsvorgängen.

Das BAMF hat mit seinem Blockchain-Projekt zur Verbesserung der Zusammenarbeit im Asylprozess gezeigt, wie ein funktionsfähiges und evaluiertes System, die behördenübergreifende Kommunikation und den sicheren und schnellen Informationsaustausch verbessert. Das BAMF nimmt bezüglich des Einsatzes der Blockchain-Technologie eine Vorreiterrolle unter den Bundesbehörden ein.

6 Thesen zum Einsatz der Blockchain-Technologie

1. Schnelligkeit: die Gesamtzeit des Prozesses kann minimiert werden. Durch die Blockchain kann stets aktuelles Wissen über den momentanen Status und die notwendigen Informationen von Vorgängen über Behördengrenzen hinweg zur Verfügung gestellt werden.
2. Integrität: Prozesse werden in der vordefinierten Weise durchgeführt. Durch die in der Blockchain hinterlegte Prozesslogik über sogenannte Smart Contracts können Prozessabweichungen vermieden bzw. vollständig dokumentiert werden.
3. Flexibilität: Blockchain-Technologien wie Hyperledger-Fabric besitzt eine modulare Architektur. Prozesse können bei neuen gesetzlichen Regelungen oder Änderungen bei eingebundenen Partnern flexibel modulunabhängig angepasst werden.
4. Sicherheit: Mit Hilfe der Blockchain-Technologie können die benötigten Daten und Informationen über Behördengrenzen hinweg verfügbar sein. Die Sicherheit, Unverfälschbarkeit, Zuordenbarkeit und der Zeitstempel ermöglichen die maximale Nachvollziehbarkeit. Dadurch liegen Informationen zur richtigen Zeit, in der erforderlichen Qualität beim richtigen Nutzer vor.
5. Kommunikation & Koordination: Jede am Blockchain-Netzwerk beteiligte Behörde erhält nahezu in Echtzeit den gleichen Sachstand zu dem ausgewählten Prozessstatus, so dass nicht immer explizit Informationen abgefragt werden müssen, und ermöglicht so einen geringeren Kommunikationsaufwand ohne damit verbundenen Fehler oder Unstimmigkeiten.
6. Nutzerzufriedenheit: Die Verwaltungsmitarbeiter haben einen Nutzen durch eine mögliche Erleichterung und Entlastung. Die Bürger erfahren zeitliche Vorteile und schnellere Entscheidungen.

Künstliche Intelligenz/Big Data

Künstliche Intelligenz & Smart/Big Data Ansätze werden heute als eine der disruptivsten Technologien der Zukunft bewertet. Ein Verständnis der damit verbundenen Chancen und Risiken aus einer menschenzentrierten Perspektive ist der Schlüssel zum Erfolg. Die Bundesregierung hat mit der Enquete-Kommission Künstliche Intelligenz und der Datenethikkommission die Grundlagen geschaffen, den komplexen Sachverhalt aus allen Aspekten zu beleuchten und zu diskutieren.

Internationale Firmen wie Google, Amazon oder Facebook haben inzwischen umfangreiche Datenpools angehäuft, die sie u.a. für ihre KI-Forschung nutzen. Vielzählige Ansätze des Maschinellen Lernens lassen sich bereits heute in Alltagsanwendungen finden, z.B. als Sprachassistenzsystem, zur Gesichtserkennung und Bildverarbeitung.

Wer führend in der KI ist, wird zukünftig wirtschaftlich führend in der Welt sein. Um dem Anspruch zu genügen, eine führende Nation der Digitalisierung zu sein, muss Deutschland in künstliche Intelligenz investieren. Die Bundesregierung muss dazu die Rahmenbedingungen schaffen.

Digitalisierung bedeutet in diesem Zusammenhang, dass Informationen, einmal erfasst, praktisch ohne Kosten beliebig vervielfältigt werden und auf die unterschiedlichste Weise für analytische Zwecke genutzt werden können. Diese sogenannten Nutzdaten werden mehr und mehr vernetzt, können somit einfach korreliert und die Erkenntnisgewinnung durch die Anwendung maschineller Verfahren (Machine Learning) exponentiell beschleunigt werden.

Aktueller Stand

Circa alle zwei Jahre, verdoppelt sich das Wissen der Menschheit. Überall entstehen neue Ökosysteme wie z.B. Blockchain, Cloud-Technologien und Shareconomy.

In der Anwendung, bietet die Künstliche Intelligenz vielzählige mathematische Verfahren und technische Lösungen, zum Vergleich sowie zur Bildung und Anwendung von Mustern. Diese Muster bilden letztlich die Wirklichkeit in bestmöglicher Form ab. Mithilfe des maschinellen Lernens werden Systeme in die Lage versetzt, auf Grundlage vorhandener Datenbestände und Algorithmen, Muster und Gesetzmäßigkeiten zu erkennen, um so Lösungen zu entwickeln.

Das beinhaltet die Abstraktion sowie Kombination von Mustern, Prüfung von Mustern gegen die Realität, Bildung neuer Muster, Update oder Verwerfung von Mustern, Vergessen von Mustern und Neubildung synaptischer Verknüpfungen. Um die Potenziale und Herausforderungen künstlicher Intelligenz zu meistern, braucht es einen Kulturwandel und Offenheit für Veränderungen. Die Attraktivität der Verwaltung muss für Bürger und Angestellte gesteigert werden. Dies erfordert die Orientierung an den Bedürfnissen der Bürger.

Im Zuge der fortschreitenden technologischen Entwicklung, müssen auch Gesetzgeber und Verwaltung Maßnahmen ergreifen, um die Basis für einen effizienten, wirksamen und ethischen Einsatz von KI in der öffentlichen Verwaltung zu gestalten.

Einsatzgebiete und Anwendungsfälle

Die öffentliche Verwaltung arbeitet im Wesentlichen auf Basis von Gesetzen, Verordnungen und Regeln. Damit eignen sich alle darauf aufbauenden Arbeiten und Vorgänge per se zur Verarbeitung und Automatisierung durch intelligente Systeme. Sofern Regelabweichungen und Ermessensspielräume zu berücksichtigen sind, können diese antrainiert werden und anschließend in die Analyse und Entscheidungsfindung einfließen. Wichtig hierbei ist zu verstehen, dass KI immer zielorientiert eingesetzt wird.

Anwendungsfälle gibt es in allen Bereichen, in denen große Datenmengen anfallen, aus denen sich Muster ableiten lassen. Die Daten liegen dafür bestenfalls bereits in elektronischer Form vor, können ansonsten auch aus unstrukturierten Daten in eine maschinenlesbare Form überführt werden.

Als wesentliche Bereiche, aus denen sich analytische Anwendungsfälle und Möglichkeiten zur KI- und Muster-gesteuerten, automatisierten Datenverarbeitung ergeben sind:

- Verkehr, (Prognosen, operative Steuerung, Planung/Simulation)
- Steuern, Gebühren, Strafen (Berechnung, Einzug, Rückerstattung, Mahnung etc.)
- Sichere Identitätsverwaltung, (Dokumente für jeweilige Lebenslagen, Anmeldungen, Zertifikate, Gesundheitsdaten, Versicherungen, Zeugnisse usw.), deren geschützter Austausch
- Serviceleistungen für Bürger (Lebenslagen/Situationen – Zustand und Veränderung wie z.B. Ausbildungsabschlüsse, Studium, Eheschließung, Kinder, Führerschein, medizinische Behandlungen, Versicherungen, etc.)
- Betrugserkennung
- Sicherheit (z.B. Identitätsfeststellung, Terrorabwehr, Datengestützte Polizeiarbeit)
- Integrative Arbeit verschiedener Abteilungen/ Bereiche (bereichsübergreifende Datenkorrelation zur Durchführung von Planungen und Simulationen)

Eine Automatisierung erzielt größte Wertschöpfung in den Bereichen:

- Antragswesen (Daten sind vorhanden und können zur maschinellen Entscheidungsfindung und Dunkelverarbeitung genutzt werden)
- Gesundheit (Analyse von Patienten- und Behandlungsdaten, Wirksamkeitsbewertung von Disease-Management-Programmen)
- Beschaffung, Dienstreisen (Planung, Durchführung, Abrechnung, Reporting)
- Compliance-Prüfungen (Mustererkennung und Transaktionsanalysen, zur Identifikation von Anomalien)
- Bürgerbeteiligung (Bürgermeinungen können jederzeit abgefragt werden)
- E-Voting

Strategische Investitionen

Laut einer aktuellen Bitkom-Umfrage sehen 62 Prozent der Bürger in Künstlicher Intelligenz eher eine Chance. Vor einem Jahr lag der Anteil noch bei 48 Prozent.

Bei der Kabinettsklausur Mitte November2018 in Potsdam hatte die Bundesregierung beschlossen, bis zum Jahr 2025 zusätzlich drei Milliarden Euro in die Entwicklung von Künstlicher Intelligenz (KI) zu investieren. Unter anderem sollen 100 neue Professuren für Künstliche Intelligenz geschaffen werde. Deutschland soll einer der führenden Standorte in Forschung und Anwendung werden.

Von der Theorie zur Praxis

Zunächst gilt es, sich auf diejenigen Anwendungsgebiete zu fokussieren, in denen sich nach Ansicht der Verwaltung neue Konzepte des Maschinellen Lernens besonders nutzbringend einbringen lassen.

Der Erfolg eines wirksamen KI- Systems, ist im Wesentlichen abhängig von der Bereitstellung einer vollständigen und, im Hinblick auf die Zielstellung, relevanten Datenbewirtschaftung.

Ist die Datenbewirtschaftung sichergestellt, können maschinelle Verfahren im Rahmen eines abgesteckten “Proof of Concept“ (POC) implementiert und auf ihre Eignung und Wirksamkeit hin überprüft werden. Dieses agile Vorgehen sichert die Erreichung der fachlichen Ziele und Einhaltung der bereitgestellten Budgets sicher. Zudem werden technische Risiken bereits in diesem frühen Stadium aufgedeckt.

Im Anschluss an einen erfolgreichen POC, lassen sich die gewonnen Ergebnisse und erlernten Modelle, z.B. auch vorab mittels eines Prototyps, auf der Gesamtdatenmenge anwenden.

Über die Initiative

Seit 2009 arbeitet eine Gruppe von IT- und Dienstleistungsunternehmen in der Initiative zusammen, um sich unter Moderation der Cyber Akademie und des Behörden Spiegels mit dem Zustand und der Weiterentwicklung von Kooperations- und Partnerschaftsmodellen zwischen öffentlichem Sektor und Privatunternehmen im IT- und Dienstleistungssektor zu befassen. In unregelmäßigen Abständen verfasst die Initiative, zu der Atos, die Bundesdruckerei, Computacenter, e-Shelter, Hewlett-Packard Enterprise, IBM und SVA zählen, Stellungnahmen und Konzeptpapiere, die dazu anregen sollen, Innovationen in organisatorischer und technischer Hinsicht als flexibles, wirtschaftliches und zukunftsorientiertes Instrument im Digitalisierungsprozess der Verwaltung zu begreifen und einzusetzen.