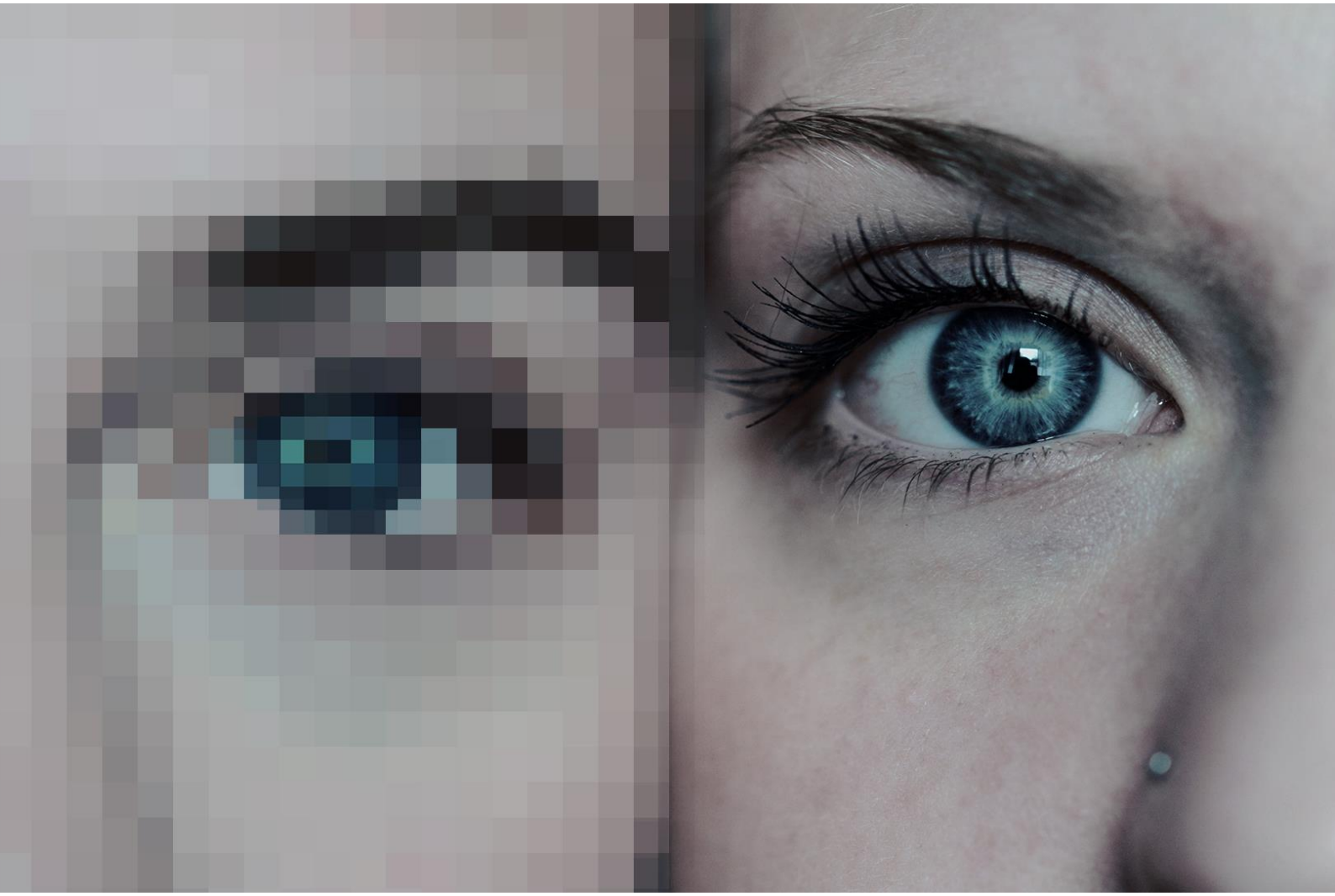
BCG

Nortal



Identifikatoren als Grundlage eines leistungsfähigen eID-Ökosystems

Die Boston Consulting Group (BCG) unterstützt führende Akteure aus Wirtschaft und Gesellschaft in partnerschaftlicher Zusammenarbeit dabei, Herausforderungen zu meistern und Chancen zu nutzen. Seit der Gründung 1963 leistet BCG Pionierarbeit im Bereich Unternehmensstrategie. Die Boston Consulting Group hilft Kunden, umfassende Transformationen zu gestalten: Die Beratung ermöglicht komplexe Veränderungen, eröffnet Wachstumschancen, schafft Wettbewerbsvorteile, verbessert die Kunden- und Mitarbeiterzufriedenheit und bewirkt so dauerhafte Verbesserungen des Geschäftsergebnisses.

Nachhaltiger Erfolg erfordert die Kombination aus digitalen und menschlichen Fähigkeiten. Die vielfältigen, internationalen Teams von BCG bringen tiefgreifende Expertise in unterschiedlichen Branchen und Funktionen mit, um Veränderungen anzustoßen. BCG verzahnt führende Management-Beratung mit Expertise in Technologie, Digital und Analytics, neuen Geschäftsmodellen und der übergeordneten Sinnfrage für Unternehmen. Sowohl intern als auch bei Kunden setzt BCG auf Gemeinschaft und schafft dadurch Ergebnisse, die Kunden nach vorne bringen. Das Unternehmen mit Büros in mehr als 90 Städten in über 50 Ländern erwirtschaftete weltweit mit 21.000 Mitarbeitern im Jahr 2019 einen Umsatz von 8,5 Milliarden US-Dollar.

Nortal ist ein multinationales Unternehmen für Strategie- und Technologieberatung. Unsere Vision ist es, eine nahtlose Gesellschaft aufzubauen. Dafür kombinieren wir unsere Erfahrungen aus der digitalen Transformation der nordeuropäischen Staaten und der Gestaltung von technologischem Wandel in Unternehmen mit einem strategischen Ansatz und datengestützter Technologie. Nortal ist in acht Ländern vertreten und beschäftigt etwa 1.000 Spezialisten, die digitale Transformationsprojekte in Europa, dem Nahen Osten, Afrika und Nordamerika durchführen.

Identifikatoren als Grundlage eines leistungsfähigen eID-Ökosystems

AUTOREN

Frank Felden
Managing Director und Senior Partner
Boston Consulting Group
Felden.Frank@bcg.com

Patrick Bauer
Associate Director, Digital Government
Boston Consulting Group
Bauer.Patrick@bcg.com

Dr. Sabine Siegert
Project Leader
Boston Consulting Group
Siegert.Sabine@bcg.com

Patrick Mesenbrock
Consultant
Boston Consulting Group
Mesenbrock.Patrick@bcg.com

Taavi Einaste
Senior Partner
Nortal
Taavi.Einaste@nortal.com

Mario Müller
Head of Digital Strategy
Nortal (vormals Schütze AG)
Mario.Mueller@schuetze.ag

Hendrik Lume
Partner, Senior Consultant
Nortal
Hendrik.Lume@nortal.com

Till Hoffmann
Consultant
Nortal
Till.Hoffmann@nortal.com

Oktober 2020

Executive Summary

Weitestgehend unbeachtet von der Öffentlichkeit wird aktuell eine der folgenschwersten Entscheidungen für die Digitalisierung in Deutschland vorbereitet. Mit dem Gesetz zur Registermodernisierung sollen Identifikatoren für natürliche Personen eingeführt werden. Identifikatoren bieten enormes Potenzial für die Verbesserung der Leistungsfähigkeit und Effizienz von Verwaltung und Wirtschaft in Deutschland. Sie sind ein wesentlicher Grundbaustein für die Digitalisierung und Voraussetzung für eine zeitgemäße Registerlandschaft, ein effizientes Interoperabilitätssystem und die Umsetzung des „Once-Only"-Prinzips. Identifikatoren bilden die Grundlage für eine Verbesserung der Datenqualität in staatlichen Registern; für die eindeutige, fehlerfreie Verknüpfung von elektronischer und physischer Identität sowie für synchrone Datenaustauschverfahren über Registergrenzen hinweg. Insbesondere Letzteres vereinfacht die Automatisierung von Prozessen und ermöglicht erhebliche Zeit- und Kosteneinsparungen für Bürger*innen, Unternehmen und die öffentliche Verwaltung. Zudem werden Innovationen in der Verwaltung, wie proaktive Verwaltungsleistungen ermöglicht. Im Zusammenspiel mit einem Interoperabilitätssystem ermöglichen Identifikatoren eine umfassende Transparenz und Datensouveränität hinsichtlich des behördenübergreifenden Austauschs personenbezogener Daten.

Gleichwohl ist die Einführung solcher Identifikatoren ein politisch und rechtlich hochsensibles Thema. In der Vergangenheit sind Versuche, Identifikatoren einzuführen, am Widerstand von Teilen der Bevölkerung und an rechtlichen Risiken gescheitert. Dabei verbietet die Rechtsprechung nicht die Einführung und Nutzung von Identifikatoren, jedoch die Zusammenführung von staatlichen Daten zu Personenprofilen. Die Rechtmäßigkeit von Identifikatoren und deren Vertrauenswürdigkeit aus Sicht der Bevölkerung hängen somit insbesondere von der Ausgestaltung der Identifikatoren und der Wirksamkeit begleitender Schutzmaßnahmen zur Verhinderung unrechtmäßiger Datenzugriffe ab. Die Ausgestaltung von Identifikatoren und verbundener Maßnahmen hat jedoch auch Auswirkungen auf sämtliche Systeme, von denen sie zukünftig verwendet werden. Je höher die Komplexität der Identifikatoren, desto höher werden sowohl die Kosten als auch die Einführungshindernisse für Datenaustauschverfahren und moderne Fachverfahren ausfallen.

Als Debattenbeitrag zur Einführung von Identifikatoren im Rahmen des Registermodernisierungsgesetzes haben BCG und Nortal ein White Paper zum deutschen eID Ökosystem erarbeitet. Identifikatoren stellen neben E-Authentifizierung und E-Signatur eines der drei Kernelemente und den Ausgangspunkt eines jeden eID-Ökosystems dar. Aufgrund der aktuellen Relevanz des Themas im Kontext der Diskussionen über ein registerübergreifendes Identitätsmanagement durch die Innenministerkonferenz stellen wir in diesem Ausschnitt aus unserem White Paper die Ergebnisse zum Thema Identifikatoren gesondert vor.

Die Möglichkeiten zur Ausgestaltung von Identifikatoren verlaufen entlang von vier wesentlichen Stellschrauben. Anhand dieser Stellschrauben lassen sich grundsätzlich zwei verschiedene Modelle identifizieren, die international verwendet werden. 21 der 22 EU-Mitgliedstaaten, die Identifikatoren für natürliche Personen nutzen, machen von einheitlichen, nicht-geheimen Identifikatoren Gebrauch. Dieses Modell bietet minimale Komplexität und ermöglicht bzw. vereinfacht eine Vielzahl von Anwendungsfällen, insbesondere die eineindeutige Verknüpfung physischer und elektronischer Identitäten. Demgegenüber verwendet Österreich als einziger EU-Mitgliedstaat ein System bereichsspezifischer, geheimer

Identifikatoren. Dieses System ist darauf ausgelegt, einen erhöhten Datenschutzstandard zu erfüllen, indem insbesondere die unrechtmäßige Zusammenführung persönlicher Daten verhindert wird. Vor dem Hintergrund des Volkszählungsurteils ist es damit als mögliches Vorbild für die Einführung von Identifikatoren in Deutschland interessant. Allerdings erhöht das österreichische Modell langfristig die Komplexität sowie die Kosten für die Erstellung verbundener Systeme und Anwendungsfälle. Zu hinterfragen ist auch der tatsächliche Nutzen des Modells hinsichtlich der effektiven Verhinderung der Zusammenführung persönlicher Daten, da in Österreich weiterhin andere Identifizierungsmerkmale, wie z. B. Namen, in dezentralen Registern gespeichert werden, die eine unrechtmäßige, manuelle Zusammenführung außerhalb des Interoperabilitätssystems ermöglichen. Für die effektive Verhütung der Zusammenführung persönlicher Daten sind Schutzmechanismen in der Registerlandschaft und im Interoperabilitätssystem bedeutender als die Ausgestaltung der Identifikatoren an sich.

Für Deutschland würde sowohl die Einführung bereichsspezifischer als auch einheitlicher Identifikatoren eine Verbesserung gegenüber dem Status quo bedeuten. Mit Blick auf den kontinuierlichen Einfluss auf Komplexität, Kosten und Erfolgschancen zukünftiger Digitalisierungsvorhaben sowie den geringen praktischen Mehrwert für den Datenschutz, den das österreichische Modell bietet, ist das Modell einheitlicher, nicht-geheimer Identifikatoren jedoch zu bevorzugen. Ein solches Modell sollte durch adäquate Schutzmechanismen gegen die unrechtmäßige Zusammenführung von persönlichen Daten begleitet werden.

Diese Schutzmechanismen sollten vor allem darauf abzielen, weitgehende Kontrolle und Transparenz über die Verwendung persönlicher Daten für Bürger*innen in einem Datenschutzcockpit zu schaffen. Grundvoraussetzung für die Einführung effektiver Schutzmechanismen zur Kontrolle registerübergreifender Datenzugriffe ist die Nutzung eines einheitlichen Interoperabilitätssystems für alle derartigen Zugriffe auf persönliche Daten. Innerhalb dieses Systems sollten rechtliche, organisatorische, prozessuale und technische Maßnahmen getroffen werden, um die Kontrolle über persönliche Daten und die Transparenz über deren Nutzung zu verankern. Zudem sollte das Modell eine einfache, rechtskonforme, sektorübergreifende Verwendbarkeit von Identifikatoren ermöglichen, um das Effizienz- und Innovationspotenzial automatischer Datenaustauschverfahren auch außerhalb der öffentlichen Verwaltung nutzbar zu machen.

Die Einführung von Identifikatoren und die damit einhergehenden Anpassungen in der Registerlandschaft und im eID-Ökosystem erfordern einen enormen Ressourcenaufwand. Dies betrifft nicht nur neu zu schaffende zentrale Stellen, sondern insbesondere auch den laufenden Aufwand für das „Record-Matching“ in dezentralen Fachregistern. Für die Einführung sollte auf geeigneter bestehender Infrastruktur aufgesetzt werden, um die Komplexität des Vorhabens zu minimieren. Die Art des Rollouts sollte abhängig von der erwarteten Nutzung für jedes Register einzeln entschieden werden - insbesondere vor dem Hintergrund, dass die Umsetzung des „Record-Matching“ für ein Land von der Größe und administrativen Unterteilung Deutschlands vermutlich mehrere Jahre in Anspruch nehmen dürfte. Für Register mit großem Potenzial für synchrone Datenaustauschverfahren, bspw. örtliche Melderegister, zentrales Fahrzeugregister und Handelsregister, könnte eine zeitnahe vollständige Ausstattung mit Identifikatoren sinnvoll sein. Auf diese Weise könnten Bürokratiekosten massiv reduziert und neuartige Ansätze, wie beispielsweise antragslose Verfahren, ermöglicht werden.

INHALTSVERZEICHNIS

Executive Summary 4

1. Einleitung: eID-Ökosysteme – ein Grundbaustein der digitalen Gesellschaft 9

4. Ganzheitliche Betrachtung von eID-Ökosystemen 15

1. Einführung: Was sind eID-Ökosysteme? 15
2. Wesentliche Bewertungskriterien von eID-Ökosystemen 21

5. Identifikatoren als Grundlage eines leistungsfähigen eID-Ökosystems 25

1. Stellschrauben zur Ausgestaltung von Identifikatoren in eID-Ökosystemen 28
2. Blick ins europäische Ausland: Ausgestaltung von Kennziffern und Auswirkungen auf das jeweilige eID-Ökosystem 34

1. Das estnische Modell 36
2. Das österreichische Modell 42
3. Interoperabilitätssysteme im Ländervergleich 47

6. Handlungsempfehlungen 51

1. Einleitung: eID-Ökosysteme – ein Grundbaustein der digitalen Gesellschaft

Die Digitalisierung ist einer der wirkungsreichsten Megatrends in Wirtschaft und Gesellschaft. Sie ist zum einen gekennzeichnet durch die beschleunigte Entwicklung und Verbreitung neuer Informations- und Kommunikationstechnologien, zum anderen durch die Substitution analoger durch digitale Prozesse. Im Ergebnis führt die Digitalisierung zu fundamentalen Veränderungen in einer Vielzahl von Lebensbereichen und Industrien. Um die digitale Transformation von Wirtschaft und Gesellschaft zu gestalten, verfügt der Staat über umfangreiche Handlungsmöglichkeiten. Diese reichen von der Schaffung grundlegender Infrastrukturen über die Förderung von Fähigkeiten sowie Investitionen bis hin zur Festlegung von Regeln und Rahmenbedingungen. Der Grad der Digitalisierung von Wirtschaft und Gesellschaft wird zunehmend zum Wettbewerbsfaktor zwischen Nationen. Daher intensivieren Regierungen weltweit ihre Bemühungen, den digitalen Wandel in der Ökonomie und der Gesellschaft erfolgreich zu gestalten.

Trotz der Fortschritte, die in den letzten Jahren erreicht wurden, hat Deutschland im gesamten Themenfeld der Digitalisierung noch erheblichen Aufholbedarf. Das gilt für die flächendeckende Bereitstellung leistungsfähiger digitaler Infrastruktur ebenso wie für die digitale Transformation insbesondere im Verwaltungs-, Gesundheits- und im Bildungsbereich.[1] Die Defizite im Hinblick auf die Digitalisierung in Deutschland sind keineswegs ein abstraktes Problem, sondern bringen gravierende Nachteile für die Bevölkerung mit sich und verursachen reale Kosten für die Wirtschaft – das führt die aktuelle globale COVID-19-Pandemie dramatisch vor Augen. Als Beispiele für technisch mögliche und dringend benötigte, aber erst in Ansätzen vorhandene Lösungen seien etwa Videosprechstunden von Ärzten inklusive der elektronischen Verschreibung von Arzneimitteln, eine sichere elektronische Identifizierung von Unternehmensvertretern bei der Online-Beantragung von staatlichen finanziellen Unterstützungen oder die einfache und geregelte Bereitstellung von Lerninhalten für Schüler*innen über das Internet genannt. Darüber hinaus könnte eine Vielzahl von digitalen Dienstleistungen die Notwendigkeit persönlicher Kontakte in Zeiten von COVID-19 minimieren. Im Verwaltungsbereich würde eine größere Anzahl vollständig digital abwickelbarer Verwaltungsleistungen eine Fülle persönlicher Kontaktpunkte überflüssig machen und das Ansteckungsrisiko vor Ort und auf den Wegen reduzieren. Leistungsfähige E-Signatur-Lösungen könnten in der Wirtschaft die Weiterführung von Unternehmensgeschäften erleichtern, z. B. durch rein digitalen Abschluss von Verträgen.

---

[1] Vgl. Europäische Kommission (2019): eGovernment Benchmark 2019; Normenkontrollrat (2019): Monitor Digitale Verwaltung #3.

Die genannten Beispiele sollen die bereits erzielten Fortschritte bei der Digitalisierung in Deutschland nicht in Frage stellen, sie machen jedoch den dringenden weiteren Handlungsbedarf deutlich. Vor diesem Hintergrund ist es von entscheidender Bedeutung, dass die Herausforderungen der Digitalisierung inzwischen auf allen Ebenen erkannt worden sind. Bund, Länder und Kommunen arbeiten in zahlreichen Initiativen daran, die Digitalisierung in Deutschland in einer Vielzahl von Bereichen voranzutreiben.

Die Digitalstrategien von Bund und Ländern als Gradmesser für die Priorisierung der Bereiche zeigen, dass vor allem vier Felder im Fokus der staatlichen Digitalisierungsbemühungen stehen: (1) der Ausbau digitaler Infrastruktur, (2) die Beschleunigung der Verwaltungsdigitalisierung, (3) die Unterstützung der Digitalisierung in Wirtschaft und Gesundheitswesen sowie (4) die Förderung der Digitalisierung im Bildungsbereich bzw. von digitalen Kompetenzen. Ein wesentliches übergreifendes Ziel staatlichen Handelns ist dabei die Bereitstellung transaktionsbasierter Dienstleistungen für Bürger und Unternehmen über das Internet (sogenannte E-Services). So sollen im Rahmen des 2017 verabschiedeten Onlinezugangsgesetzes (OZG) bis Ende 2022 knapp 600 Verwaltungsleistungen online angeboten werden. Im Gesundheitsbereich sollen Patienten zunehmend über das Internet von Ärzten beraten werden, elektronische Arzneimittelrezepte und Verordnungen auf digitalem Wege erhalten und auf ihre Patientendaten online zugreifen können. Auch im Bildungsbereich sollen u. a. Lerninhalte verstärkt über das Internet angeboten werden.

Ohne eine sichere und leistungsfähige eID-Lösung für die Ermöglichung und Nutzung von E-Services ist jedoch eine Vielzahl der genannten Ziele, allen voran die Umsetzung des OZG, nicht zu erreichen.

Der Begriff „eID“ wird zumeist allein mit Bezug auf Mittel der E-Authentifizierung[2], wie den elektronischen Personalausweis, verwendet. So konzentriert sich die eID-Strategie des IT-Planungsrates aus dem Jahr 2013 hauptsächlich auf die elektronischen Verfahren zur Identifizierung und Signatur mit dem Ziel, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit von elektronischen Transaktionen zu gewährleisten.[3] Tatsächlich umfasst der eID-Themenkomplex jedoch weitere wichtige, in wechselseitiger Abhängigkeit zueinander stehende Elemente, die einer ganzheitlichen Betrachtung bedürfen. Um sowohl die Digitalisierung von Wirtschaft und Gesellschaft voranzutreiben als auch die erfolgreiche Umsetzung des OZG sowie die verstärkte Nutzung der Online-Angebote im Gesundheits-, Bildungs- und in weiteren Lebensbereichen sicherzustellen, kommt es wesentlich auf die Ausgestaltung dreier Elemente an.

---

[2] Der Begriff „E-Authentifizierung“ wird hier zu Vereinfachungszwecken synonym mit den Begrifflichkeiten „elektronische Identifizierung“ und „Authentifizierung“ nach eIDAS verwendet.

[3] IT-Planungsrat (2013): Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie), Version 1.0 – Beschlussfassung 12. Sitzung IT-Planungsrat am 02.10.2013.

Diese prägen zusammen maßgeblich die Beschaffenheit des gesamthaften „eID-Ökosystems“ in Deutschland:

1. **Identifikatoren**[4]
   (Personen-)Kennziffern bilden das Fundament jedes eID-Ökosystems, indem sie die eineindeutige Verknüpfung physischer und elektronischer Identitäten ermöglichen. Weiterhin dienen sie als Grundlage für die Vereinfachung von E-Authentifizierung, Datenaustauschverfahren, medienbruchfreien Prozessen und die Umsetzung des „Once-Only“-Prinzips zur einmaligen Erfassung von Datenpunkten.[5]
2. **E-Authentifizierung**
   „E-Authentifizierung“ ist der sichere elektronische Nachweis der eigenen Identität und stellt die Grundlage für die Nutzung sensibler Services über das Internet dar.
3. **E-Signatur**
   „E-Signatur“ bezeichnet die elektronische Abgabe rechtsverbindlicher Willenserklärungen und ist notwendig, um Rechtsgeschäfte über das Internet zu ermöglichen bzw. entscheidend zu vereinfachen.

Aktuell gibt es in Deutschland keinen weithin nutzbaren eindeutigen Identifikator für natürliche Personen. Die Bundesregierung arbeitet jedoch aktiv an der Einführung und will im ersten Halbjahr 2020 einen Gesetzentwurf dazu einbringen. Die Grundlage für eine sichere E-Authentifizierung für alle Bürger*innen wurde mit der Einführung des elektronischen Personalausweises im Jahr 2010 geschaffen. Die tatsächliche Nutzung ist jedoch ebenso wie die Zahl der Diensteanbieter zur Verwendung der Online-Ausweisfunktion gering. Aus diesem Grund sowie infolge des technischen Fortschritts gibt es sowohl privatwirtschaftliche als auch staatliche Initiativen mit dem Ziel, alternative Methoden zur E-Authentifizierung zu schaffen. Im Hinblick auf die E-Signatur war Deutschland in den 1990er Jahren noch Vorreiter bei der Schaffung rechtlicher Rahmenbedingungen für deren Einführung. Im Gegensatz zu anderen europäischen Ländern hat sich die E-Signatur hierzulande in der breiten Bevölkerung aber bis heute nicht durchsetzen können. Ihre gesellschaftlichen Potenziale bleiben dadurch bislang weitgehend ungenutzt.

Im Ergebnis weist das deutsche eID-Ökosystem als Grundbaustein für die Digitalisierung von Staat, Wirtschaft und Gesellschaft noch eine Reihe großer Lücken und Schwachstellen auf. Um die Digitalisierung effizient voranbringen zu können, müssen diese Lücken geschlossen werden.

---

[4] In diesem White Paper wird der Terminus „Identifikator“ als Oberbegriff für Kennziffern zur eindeutigen Identifizierung von Individuen in behördlichen oder privaten Interaktionen gebraucht. In anderen Publikationen verwendete Synonyme sind beispielsweise „Identifier“ oder „(Personen-)Kennziffer“.

[5] Zudem ist die Ausgestaltung von eindeutigen elektronischen Identifikatoren für alle gesellschaftlich relevanten Objekte (wie z. B. Unternehmen, Fahrzeuge, Wohnungen oder Flurstücke) im Rahmen der Registermodernisierung in Deutschland relevant. Im Rahmen dieses Papers wird der Fokus jedoch allein auf Identifikatoren für natürliche Personen gelegt.

Im vorliegenden White Paper wird die Rolle von Identifikatoren im eID-Ökosystem analysiert und gezeigt, welche grundsätzlichen Handlungsoptionen der Staat zur Ausgestaltung von Identifikatoren hat, welche Ansätze sich in anderen europäischen Staaten bewährt haben und welche Fallstricke es zu vermeiden gilt. Darauf aufbauend werden Handlungsempfehlungen zur Gestaltung von Identifikatoren als Grundlage für ein funktionierendes deutsches eID-Ökosystem entwickelt. Mit diesen Handlungsempfehlungen wollen wir Impulse für das weitere Gesetzgebungsverfahren und die öffentliche Debatte zum Registermodernisierungsgesetz sowie zur Realisierung eines leistungsstarken eID-Ökosystems in Deutschland geben, das auf die Schaffung eines hohen Mehrwerts für die Bürger*innen durch effiziente, benutzerfreundliche und einfache Interaktion mit staatlichen und privaten Akteuren ausgerichtet ist und zugleich deutsche und europäische Datenschutzstandards berücksichtigt.

4. Ganzheitliche Betrachtung von eID-Ökosystemen

1. Einführung: Was sind eID-Ökosysteme?

Die Verbreitung und Weiterentwicklung des Internets ermöglichen es, eine wachsende Zahl von staatlichen und privaten Leistungen online anzubieten. Diese reichen von der einfachen Bereitstellung von Informationen über unterschiedliche Interaktionsmöglichkeiten bis hin zu vollständig online durchführbaren Transaktionen. Während die Informationsbereitstellung im Internet nicht viel mehr als eine Website erfordert und Interaktionsangebote, z. B. über ausfüllbare Formulare oder Chats, relativ einfach umsetzbar sind, müssen für die Durchführung von Transaktionen über das Internet zusätzliche Voraussetzungen geschaffen werden. Dies gilt insbesondere für Transaktionen, in denen sensible, personenbezogene Daten verarbeitet werden, wie z. B. beim Online-Banking, bei elektronischen Verwaltungs- oder Gesundheitsleistungen.

Genau wie in der physischen Welt muss bei solch sensiblen Transaktionen im Internet die Identität der Beteiligten sichergestellt (E-Authentifizierung) und mit bestehenden personenbezogenen Daten abgeglichen werden („Record-Matching" mittels Identifikatoren). Gegebenenfalls ist zusätzlich die Abgabe rechtsverbindlicher Willenserklärungen erforderlich (E-Signatur). Die Ausgestaltung dieser drei Elemente – Identifikatoren, E-Authentifizierung und E-Signatur – sowie alle mit diesen Elementen verbundenen elektronischen Identifizierungsmittel, Vertrauensdienste und Diensteanbieter können vereinfachend als „eID-Ökosystem" bezeichnet werden. Darin bilden Identifikatoren, E-Authentifizierung und E-Signatur die Grundvoraussetzung für die einfache Durchführung von sensiblen Transaktionen im Internet.

Auf staatlicher Ebene bedeutet dies, dass sich die Digitalisierung in Wirtschaft und Gesellschaft ohne ein funktionierendes eID-Ökosystem nur schwer voranbringen lässt. Kritische Digitalisierungsinitiativen in Deutschland, wie das OZG oder die Digitalisierung im Gesundheitswesen, können ohne eine Weiterentwicklung des deutschen eID-Ökosystems kaum erfolgreich sein. Dies betrifft die Nutzung der zu erstellenden E-Services, die funktionierender Methoden zur E-Authentifizierung bedürfen, sowie die E-Signatur, deren flächendeckender Gebrauch die Rechtssicherheit von Transaktionen im Internet deutlich erhöhen und deren Kosten senken könnte. Dabei hängt der mögliche Grad der Automatisierung von E-Services – und damit die Realisierung von Effizienzpotenzialen durch die Digitalisierung – maßgeblich von einem robusten Identifikatorensystem ab, das einen rechtskonformen automatisierten Datenaustausch über Organisationsgrenzen hinweg vereinfacht.[6]

---

[6] Aus diesem Grund wird im vorliegenden White Paper im Rahmen der Diskussion von Identifikatoren auch auf den an das eID-Ökosystem angrenzenden Bereich der Interoperabilität eingegangen. „Interoperabilität" bezieht sich auf

Um die Elemente des eID-Ökosystems in ihrer Gesamtheit einfacher nachvollziehen zu können und fachbezogene Begrifflichkeiten korrekt einzuordnen, stellt Abbildung 1 die Elemente des eID-Ökosystems und dessen angrenzende Bereiche dar. Der Identifikator ist zentrales Verknüpfungselement zwischen physischer und elektronischer Identität. Ferner nimmt er eine zentrale Rolle in der eindeutigen Verknüpfung zwischen elektronischer Identität und den in den Datenbanken und Registern der Diensteanbieter hinterlegten personenbezogenen Daten ein.

Elektronische Identifizierungsmittel sind die Plattform, die Personen für E-Authentifizierung und E-Signatur bei Diensteanbietern nutzen können. In engem Zusammenhang mit dem eID-Ökosystem steht der Bereich der Interoperabilität. Ein Interoperabilitätssystem übermittelt Daten auf sicherem und standardisiertem Wege zwischen Diensteanbietern. Auch hier spielen Identifikatoren eine zentrale Rolle, indem sie eine effiziente Verknüpfung von personenbezogenen Daten ermöglichen. Zudem können in Interoperabilitätssystemen ein Datenschutzcockpit und ein Konsensmodul eingesetzt werden, um die Nachvollziehbarkeit von Datenflüssen und die Kontrolle über Datenzugriffe für Bürger*innen sicherzustellen. In diesem Kontext sind die Begriffe Transparenz („Ich kann nachvollziehen …“) und Datensouveränität („Ich erlaube …“) von zentraler Relevanz.

---

eine standardisierte Verknüpfung von Informationssystemen innerhalb von Organisationen sowie über Organisationsgrenzen hinweg, um einen einfachen Austausch von Informationen zu ermöglichen und dadurch u. a. Geschäftsprozesse effizienter gestalten zu können. Damit in Verbindung stehen Möglichkeiten für die Bürger*innen, dem Austausch der Daten über ein Konsensmodul zuzustimmen und über ein Datenschutzcockpit den Austausch der Daten nachzuvollziehen.

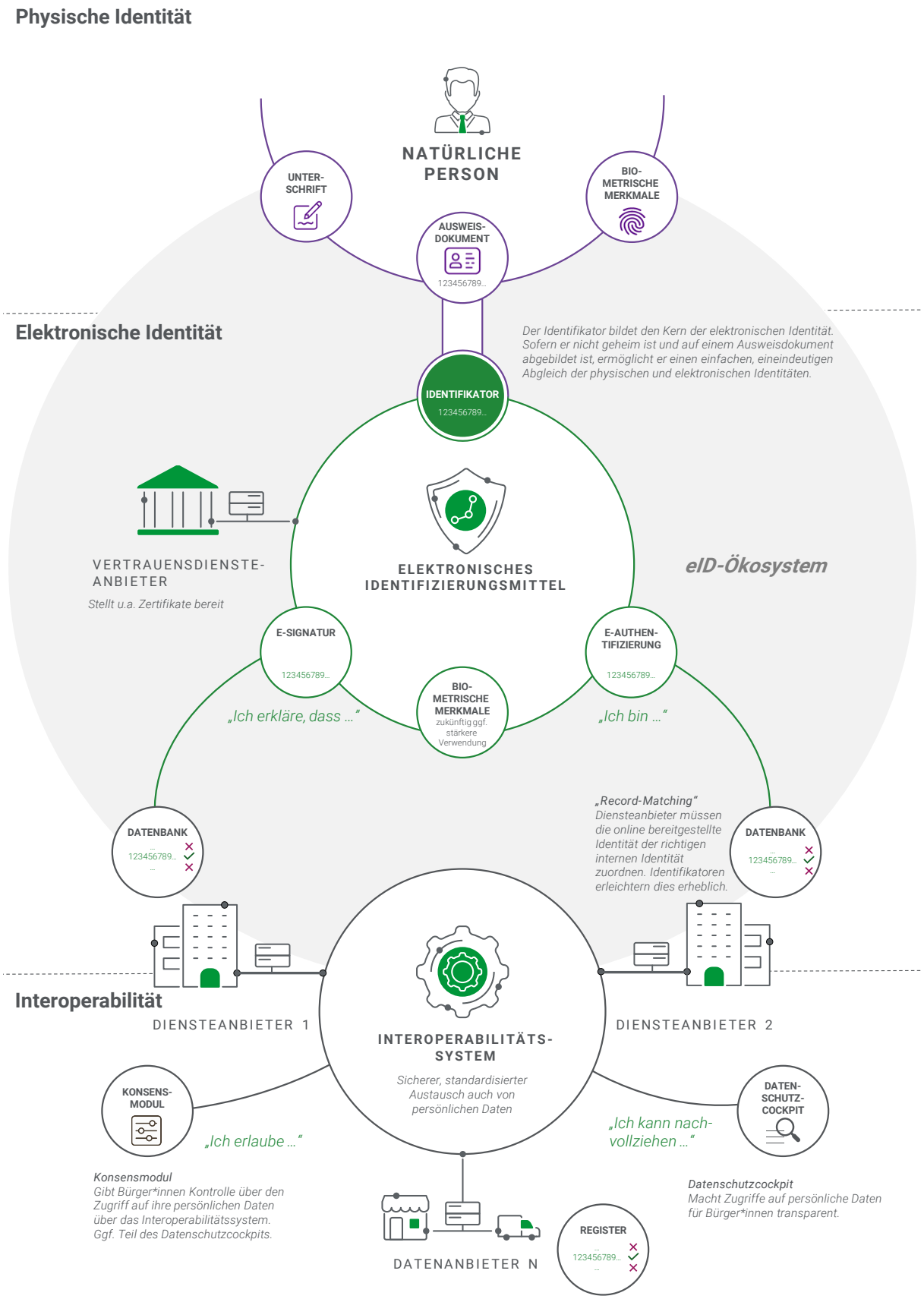


Abbildung 1: Darstellung des eID-Ökosystems und angrenzender Bereiche

Im Hinblick auf die Bereitstellung staatlicher Dienstleistungen und insbesondere die Umsetzung des OZG verdeutlicht das Reifegradmodell digitaler Verwaltungsleistungen (siehe Abbildung 2) die entscheidende Rolle des eID-Ökosystems (sowie des Interoperabilitätssystems) für die erfolgreiche Digitalisierung der Verwaltung.

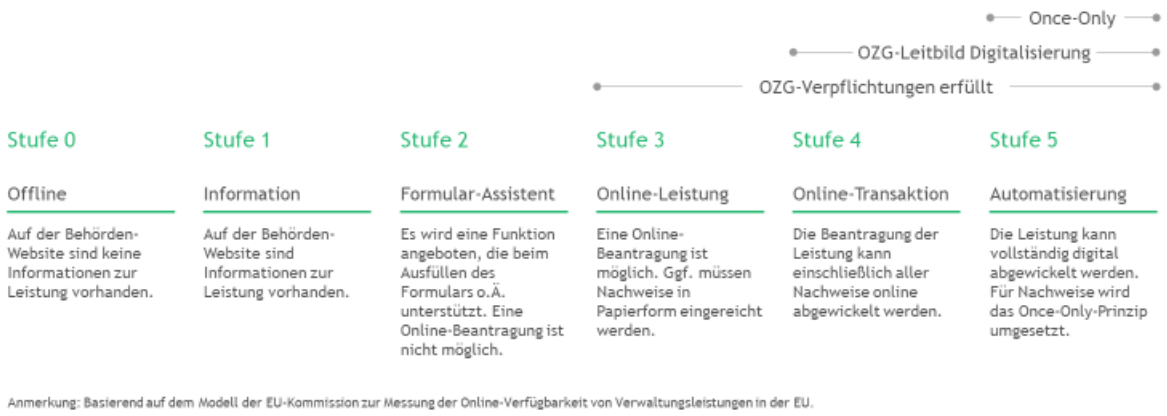


Abbildung 2: Reifegradmodell digitaler Verwaltungsleistungen nach OZG

Die Wahrnehmung digitaler Angebote wie der Online-Einsicht in die Öffnungszeiten des örtlichen Bürgeramtes (Stufe 1 – Information) oder des Herunterladens eines Formulars zum Ausdruck und zur analogen Weiterverarbeitung (Stufe 2 – Assistenz) kann ohne elektronische Identitätsnachweise erfolgen, da hier lediglich öffentliche Informationen verarbeitet und für Bürger*innen leichter zugänglich gemacht werden. Hingegen ist für Online-Leistungen ab Stufe 3 der elektronische Nachweis der Identität (E-Authentifizierung) erforderlich. Je nach Sensibilität der E-Services ändert sich die Anforderung an das Vertrauensniveau der E-Authentifizierung und damit auch der zulässigen elektronischen Identifizierungsmittel. Im Falle von E-Services, die ein hohes Vertrauensniveau erfordern, ist in Deutschland nur der elektronische Personalausweis[7] als Identifizierungsmittel zulässig. Dies verdeutlicht die Abhängigkeit der möglichen Nutzung solcher E-Services von der Verbreitung und Annahme von Identifizierungsmitteln, insbesondere dem Personalausweis.

Die Verwendung von E-Signaturen kann die Umsetzung von E-Services erheblich vereinfachen, da qualifizierte elektronische Signaturen gleichwertig mit handschriftlichen Unterschriften sind. Bei einer allgemeinen Akzeptanz und Berücksichtigung der qualifizierten E-Signatur durch alle Behörden wären z. B. keine weiteren Gesetzesänderungen notwendig, um elektronisch signierte Anträge zu akzeptieren. In der deutschen öffentlichen Verwaltung wird durch eine entsprechende Regelung im E-Government-Gesetz die E-Authentifizierung mit dem Personalausweis als

[7] Bzw. die eID-Karte für Unionsbürger*innen oder der elektronische Aufenthaltstitel für Zugewanderte aus Drittstaaten.

technologisches Äquivalent der qualifizierten E-Signatur angesehen. Dies hat jedoch keine Gültigkeit für Transaktionen in anderen Sektoren oder außerhalb der nationalen behördlichen Serverumgebung.

Zugleich muss bei der E-Authentifizierung die auf dem Identifizierungsmittel gespeicherte Identität mit der passenden Identität in den Datenbeständen des Diensteanbieters abgeglichen werden (Record-Matching). Dieser Prozess lässt sich durch die Verwendung eineindeutiger Identifikatoren erheblich vereinfachen.

Die Bedeutung von Identifikatoren und ihres Effekts für ein vereinfachtes Record-Matching erhöht sich nochmals für Transaktionen ab der Stufe 5. Bei diesen Transaktionen müssen als Teil der Verwaltungsleistung Informationen mehrerer staatlicher Informationsgeber kombiniert werden, z. B. bei der Beantragung von Ausbildungsförderung. Hierfür ist zusätzlich zur Möglichkeit der E-Authentifizierung auch die Interoperabilität, also die reibungslose Weitergabe und Verknüpfung von Informationen aus verschiedenen Registern und Datenbanken, erforderlich. Dazu müssen Daten aus verschiedenen Quellen, ggf. unabhängig von elektronischen Identifizierungsmitteln, derselben Identität zugewiesen werden, damit die richtigen Daten übertragen werden. Durch eineindeutige Identifikatoren wird dies erheblich vereinfacht. Dadurch können Verwaltungsleistungen vollständig automatisiert und die Bürger*innen und die Verwaltung von einem Maximum an Bearbeitungsaufwand entlastet werden. Ein Beispiel hierfür ist die automatische Befüllung einer Steuererklärung inklusive aller Informationen, die bereits bei anderen staatlichen Stellen vorliegen. Während im Reifegradmodell digitaler Verwaltungsleistungen die Abhängigkeit der staatlichen Digitalisierung von der Ausgestaltung des eID-Ökosystems dargestellt wird, gilt diese grundsätzliche Dynamik ebenso für den Privatsektor. Auch hier war und ist beispielsweise das Vorhandensein sicherer Verfahren zur E-Authentifizierung elementare Vorbedingung für die Etablierung sensibler E-Services wie z. B. des Online-Bankings.

Für die Weiterentwicklung der drei grundlegenden Elemente von eID-Ökosystemen – Identifikatoren, E-Authentifizierung und E-Signatur – ist die Betrachtung zweier weiterer Aspekte wichtig: erstens der **Interdependenzen** zwischen den Elementen des eID-Ökosystems und zweitens der **Dynamiken der Plattformökonomie**, die über den Erfolg oder Misserfolg von elektronischen Identifizierungsmitteln mitentscheiden.

Die **starken Interdependenzen** zwischen den verschiedenen eID-Elementen unterstreichen die Notwendigkeit einer ganzheitlichen, ressortübergreifenden Betrachtung des gesamten eID-Ökosystems. Dies kann am Beispiel der geplanten Einführung eines personenbezogenen Identifikators in Deutschland illustriert werden. Eine solche Einführung würde etwa umfangreiche Anpassungen in der deutschen staatlichen Registerlandschaft erfordern und zwangsläufig Einfluss auf die Ausgestaltung des elektronischen Personalausweises haben. Sollte

es sich um einen nicht-geheimen Identifikator handeln, könnte über zusätzliche Datenschnittstellen auf dem Personalausweis für privatwirtschaftliche Anwendungsfälle nachgedacht werden, z. B. die Codierung des Identifikators in einem Barcode auf dem Ausweis. Hierdurch könnte das Dokument einfacher als Kunden- oder Bonuskarte verwendet und zusätzlicher Nutzen für Bürger*innen und Wirtschaft gestiftet werden. Des Weiteren müsste ein nicht-geheimer Identifikator auch bei bestehenden und neuen E-Signatur-Lösungen berücksichtigt werden und würde die eineindeutige Verknüpfung einer E-Signatur zu einer physischen Identität vereinfachen. Zusätzlich kann z. B. die kostenlose Beinhaltung von E-Signaturen in Mitteln zur E-Authentifizierung, wie dem elektronischen Personalausweis, die Attraktivität von E-Signaturen für Bürger*innen sogar dann steigern, wenn die E-Authentifizierung selbst nur für wenige E-Services nutzbar ist.

Neben der Berücksichtigung von Interdependenzen zwischen den Elementen des eID-Ökosystems sind **plattformökonomische Dynamiken** zentral für Erfolg oder Misserfolg von eID-Ökosystemen. Dies betrifft insbesondere die Elemente E-Authentifizierung und E-Signatur und die mit ihnen verbundenen elektronischen Identifizierungsmittel.[8] Als Geschäftsmodell liegen solchen elektronischen Identifizierungsmitteln sogenannte Multi-sided Platforms (vgl. Abbildung 3) zugrunde. Denn elektronische Identifizierungsmittel bringen Nutzer mit verifizierten Identitäten mit Diensteanbietern zusammen, die das Identifizierungsmittel zur E-Authentifizierung und/oder E-Signatur in ihren E-Service integrieren. Solche Plattformen weisen starke Netzwerkeffekte auf, da ihr Wert sich mit steigender Anzahl von Nutzern bzw. Diensteanbietern für alle Parteien deutlich erhöht. Gleichzeitig können sie nur dann erfolgreich sein, wenn eine kritische Masse von Bürger*innen und Diensteanbietern die Plattform bzw. das Identifizierungsmittel verwendet. Die Lösung dieses Henne-Ei-Dilemmas der Plattformökonomie stellt für Anbieter von elektronischen Identifizierungsmitteln in Deutschland bis heute die größte Herausforderung dar. Auch 10 Jahre nach der Einführung des Personalausweises mit eID Funktion ist es in Deutschland nicht gelungen ein flächendeckendes eID-Ökosystem zu errichten, welches Anreize zur Nutzung für Bürger*innen und Anbieter gleichermaßen schafft. Obwohl höchste Datenschutz- und Sicherheitseigenschaften implementiert wurden, bleibt das Henne-Ei-Dilemma maßgeblich für die bis heute geringe Nutzungsbilanz. Zugleich wird die staatlich-gesicherte, elektronische Identifizierungslösung insbesondere im privatwirtschaftlichen Bereich durch weniger sichere Alternativen unterlaufen.

---

[8] Zusätzlich gilt dies zumindest teilweise auch für den an das eID-Ökosystem angrenzenden Bereich der Interoperabilität. Denn auch bei Interoperabilitätssystemen gibt es zwei Parteien, die über das System miteinander interagieren – Datenanbieter und Datenkonsumenten. Zwischen ihnen treten starke Netzwerkeffekte auf. Das bedeutet, dass der Anreiz, dem Interoperabilitätssystem beizutreten, insbesondere mit der Anzahl der Datenanbieter steigt.

In den letzten Jahrzehnten hat die Plattformökonomie stark an Bedeutung gewonnen und sie kann auf das eID-Ökosystem übertragen werden. Daraus lassen sich wichtige Erkenntnisse darüber ableiten, wie Plattformen zum Erfolg geführt werden können. Auch der Staat muss diesen Aspekt bei der Ausgestaltung des eID-Ökosystems zwingend berücksichtigen.

Abbildung 3: Elektronische Identifizierungsmittel als Multi-sided Platforms

2. Wesentliche Bewertungskriterien von eID-Ökosystemen

Um eID-Ökosysteme analysieren und vergleichen zu können, sind Bewertungskriterien erforderlich, die sich auf verschiedene Elemente nationaler Ökosysteme gleichermaßen anwenden lassen. Durch eine ganzheitliche Betrachtung der Bewertungskriterien für die Elemente eines eID-Ökosystems kann festgestellt werden, welchen Nutzen ein solches System dem Staat, den Bürger*innen sowie Unternehmen bietet. In diesem White Paper betrachten wir die drei qualitativen Kriterien, die sich für die Bewertung der Leistungsfähigkeit von eID-Ökosystemen als besonders aussagekräftig erwiesen haben: (1) Nutzbarkeit, (2) Einfachheit und (3) Vertrauenswürdigkeit.

Der Grad der **(1) Nutzbarkeit** gibt an, inwieweit ein Element des eID-Ökosystems für alle Beteiligten und über Bereiche oder Dienste hinweg anwendbar ist. Bei Identifikatoren bezieht sich dies beispielsweise darauf, ob sie sowohl bereichsübergreifend innerhalb der Verwaltung, sektorübergreifend zwischen öffentlichen und privaten Akteuren wie auch grenzübergreifend nutzbar sind. Im Hinblick auf E-Authentifizierung und E-Signatur betrifft dieses Kriterium hauptsächlich den Umfang der Nutzbarkeit des verwendeten elektronischen Identifizierungsmittels. Das gilt zum einen für die Nutzerseite, für welche die Anzahl der

Diensteanbieter maßgeblich die Nutzbarkeit beeinflusst, wie auch zum anderen für die Diensteanbieter selbst, für die wiederum die Anzahl der Nutzer ausschlaggebend für die Nutzbarkeit des Identifizierungsmittels ist. Bei der elektronischen Signatur spielt zudem die Akzeptanz der verwendeten E-Signatur eine Rolle.

Als zweites Kriterium betrachten wir die **(2) Einfachheit** der Elemente des Ökosystems. Hier wird bewertet, wie einfach oder kompliziert sich die Nutzung des eID-Elements sowohl für Bürger*innen als auch für Diensteanbieter gestaltet. Faktoren, die für die Benutzerfreundlichkeit berücksichtigt werden, sind etwa der Bedarf an notwendigen Endgeräten für elektronische Identifizierungsmittel, wie z. B. Kartenlesegeräte, sowie die Existenz und Ausgestaltung von Online-Lösungen – beispielsweise Desktopanwendungen, browserbasierten Lösungen oder auf Mobilgeräten nutzbaren Anwendungen (Mobile Friendliness). Maßgebend ist zudem die Unkompliziertheit der Registrierung und Inbetriebnahme des elektronischen Identifizierungsmittels – sowohl für die Nutzer als auch die Diensteanbieter.

Weiterhin können Elemente des eID-Ökosystems anhand des Niveaus der **(3) Vertrauenswürdigkeit** verglichen und bewertet werden. Dieses Kriterium beurteilt einzelne Elemente des untersuchten eID-Ökosystems im Hinblick auf Aspekte der Sicherheit, Transparenz und des Datenschutzes. Die Sicherheit elektronischer Identifizierungsmittel lässt sich insbesondere anhand des gewährleisteten Vertrauensniveaus für E-Authentifizierung und E-Signatur einschätzen (gemessen an nationalen und internationalen Standards). Bei Identifikatoren bezieht sich dies hauptsächlich auf ihre Verschlüsselung und Segmentierung. Die Faktoren Transparenz und Datenschutz beschreiben, inwieweit und auf welche Weise Bürger*innen Kontrolle und Überblick darüber besitzen, welche ihrer Daten zu welchem Zeitpunkt welcher Stelle zugänglich gemacht werden. Dies betrifft zum einen das Ausmaß, in welchem Bürger*innen die Weitergabe von Daten im Rahmen der Verwendung elektronischer Identifizierungsmittel selbst zu kontrollieren vermögen, indem sie etwa zu übertragende Informationen (de)selektieren können. Zum anderen umfasst dieses Bewertungskriterium auch die Möglichkeit für Bürger*innen, Einblick darin zu nehmen, welcher Akteur auf welche Daten Zugriff erhalten hat und wann er diese nutzt.

Die qualitativen Bewertungskriterien stehen teilweise in einem Konkurrenzverhältnis zueinander und sind deshalb in ihrer Gesamtheit zu betrachten. So führt beispielsweise die Optimierung eines Kriteriums nicht zwingend zu einem optimalen Gesamtergebnis. Das größte Konfliktpotenzial besteht zweifellos zwischen Nutzbarkeit und Einfachheit auf der einen Seite und Vertrauenswürdigkeit auf der anderen. Wie dieser Konflikt für die einzelnen Elemente des eID-Ökosystems in unterschiedlichen Ländern gelöst werden konnte und welche Vor- und Nachteile die jeweiligen Modelle charakterisieren, wird in den folgenden Betrachtungen zu den Ausgestaltungsmöglichkeiten verschiedener Elemente des eID-Ökosystems untersucht.

5. Identifikatoren als Grundlage eines leistungsfähigen eID-Ökosystems

Die Modernisierung der deutschen staatlichen Registerlandschaft und die Einführung eines für E-Authentifizierung nutzbaren und über Register und Sektoren hinweg verknüpfbaren Identifikators bieten einen enormen Mehrwert für die Bürger*innen und großes wirtschaftliches Potenzial.[9] Identifikatoren bilden die Grundlage für effiziente und eindeutige sowie den Anforderungen der Nutzbarkeit und Einfachheit entsprechende Authentifizierungs-, Signatur- und Datenaustauschprozesse innerhalb eines eID-Ökosystems.

Im Kontext aktueller Reformüberlegungen über eine zeitgemäße Ausgestaltung von Identifikatoren und eines eng damit verbundenen Interoperabilitätssystems sprechen vier Hauptargumente für die Einführung eines Identifikator- und Interoperabilitätssystems. Das ist zunächst eine **(1) eindeutige, fehlerfreie Verknüpfung von Identitäten und Daten** sowie **(2)** die **Effizienzsteigerung von Datenaustauschprozessen**. Vorteile für die Bürger*innen bestehen insbesondere in der **(3) Zeitersparnis im Rahmen von Dienstleistungen** sowie in der **(4) Schaffung von Transparenz und Datensouveränität** im Kontext datenschutzrechtlicher Anforderungen.

Wie in Abbildung 1 (Gesamtüberblick des eID-Ökosystems) dargestellt wird, bildet der Identifikator die Grundlage für eine **(1) eindeutige, fehlerfreie Verknüpfung** von elektronischer und physischer Identität sowie von elektronischer Identität mit personenbezogenen Daten aus den Datenbanken innerhalb des eID-Ökosystems sowie innerhalb eines Interoperabilitätssystems. Durch die eindeutige Verknüpfung von Daten und Identitäten können Verwechslungen und die fehlerhafte Verwendung von Daten Unbeteiligter verhindert werden. Dies bedeutet zum einen, dass digitale Prozesse und Dienstleistungen dank eindeutiger Zuordnungen nicht mehr unterbrochen und manuell korrigiert werden müssen. Zum anderen wird für die Bürger*innen eine Leistungsgerechtigkeit sichergestellt, indem Ansprüche auf staatliche Zuwendungen eindeutig erkannt werden können.

Indem Identifikatoren Identitäten und Daten miteinander verknüpfen, erhöht sich entsprechend die Datenqualität innerhalb der Datenbanken. Die damit erreichte hohe Validität und Konsistenz der Daten **(2) steigert die Effizienz von Datenaustauschprozessen** auf Grundlage des Interoperabilitätssystems und ermöglicht dadurch vor allem einen synchronen Datenaustausch.

---

[9] Wie auch in einem Gutachten des Normenkontrollrats im Jahr 2017 festgestellt wurde, bildet eine moderne Registerlandschaft die Basis für effiziente, bürger- und unternehmensfreundliche digitale Verwaltungsdienstleistungen. Vgl. Normenkontrollrat (2017): Mehr Leistungen für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.

Somit können medienbruchfreie, automatisierte Prozesse ohne manuelles Eingreifen gewährleistet werden.

Die bereits genannten Vorteile zur Identität-Daten-Verknüpfung sowie zur Effizienzsteigerung von Datenaustauschprozessen wirken sich unmittelbar auf die **(3) Zeitersparnis im Rahmen von Dienstleistungen** für Bürger*innen und die Verwaltung aus. Behördendienstleistungen können auf Grundlage eines behördenübergreifenden Datenaustauschs medienbruchfrei abgewickelt und dadurch die Bearbeitungszeit sowohl der Bürger*innen als auch der Verwaltung minimiert werden.

Dank der Einführung von Identifikatoren und eines Interoperabilitätssystems wird eine umfassende **(4) Transparenz und Datensouveränität** hinsichtlich des behördenübergreifenden Austauschs personenbezogener Daten einfacher möglich. Die Einführung von Identifikatoren begünstigt die Schaffung eines einheitlichen Interoperabilitätssystems, welches als Governance-Institution den Bürger*innen u. a. Transparenz und Kontrolle über behördenübergreifende Datenzugriffe ermöglichen kann. Dadurch lässt sich das datenschutzrechtliche Risiko unautorisierter und umfassender Profilbildung minimieren.

Wenngleich die aktuellen Bestrebungen von Bund und Ländern, umfassende Reformen der Registerlandschaft und des Identitätsmanagements durchzuführen, notwendige Schritte im Zuge der Digitalisierung darstellen, ist die Diskussion um die Einführung eines Identifikators für natürliche Personen keineswegs neu. Die heutige Infrastruktur der staatlichen Identifikation von Individuen und der Ausgestaltung von Identifikatoren ist in großen Teilen ein Ergebnis der kontroversen Debatten um Volkszählung und Rasterfahndung in den 1970er und 1980er Jahren. Die 1964 zusammen mit der elektronischen Datenverarbeitung von den Trägern der gesetzlichen Rentenversicherung eingeführte Rentenversicherungsnummer (RV-Nummer) entwickelte sich in den Folgejahren schleichend zu einem sektorübergreifenden Identifikator. Bis zum Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 bedienten sich Krankenkassen, Behörden und Unternehmen der RV-Nummer als eines einheitlichen Identifikators. Ergänzend zur Rentenversicherungsnummer gab es ab 1973 erste Bestrebungen, personenbezogene Basisdaten der Bürger*innen zu zentralisieren und mit einem Personenkennzeichen zu verknüpfen.

Im Mittelpunkt der Verfassungsbeschwerden gegen das Volkszählungsgesetz, die zu der Grundsatzentscheidung des Bundesverfassungsgerichts führten, stand der Versuch, die statistische Datenerhebung mit einem Melderegisterabgleich zu koppeln. Die Kernprinzipien des Urteils sind bis heute in den Systemen zu Datenerfassung, Datenaustausch und Datenverarbeitung verankert. Sie können im Wesentlichen in drei Hauptprinzipien aufgeteilt werden: **(1) das Verbot der staatlichen Speicherung höchstpersönlicher Daten**, **(2) das Verbot der (anlasslosen) Profilbildung** sowie **(3) das Recht auf informationelle Selbstbestimmung**. Alle

drei Prinzipien beruhen auf der Annahme, dass es kein belangloses Datum gibt. Mit dem Urteil wurde das Grundrecht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts (GG Art. 2) geprägt.

Die Einführung eines Identifikators für natürliche Personen wird durch das Volkszählungsurteil nicht direkt verboten, untersagt wird darin jedoch die Zusammenführung von persönlichen Daten zum Zweck der Erstellung von Persönlichkeitsprofilen. Entsprechend gibt es keine konkreten rechtlichen Vorgaben dazu, welche Arten von Identifikatoren rechtlich zulässig sind. Folglich besteht Unsicherheit darüber, wie genau ein solcher Identifikator und flankierende Maßnahmen zur Verhinderung der Bildung von Persönlichkeitsprofilen ausgestaltet sein müssen, um einer rechtlichen Prüfung durch die deutsche Gerichtsbarkeit standzuhalten.[10] Grundsätzlich lässt sich sagen, dass die Einführung eines Identifikators einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen würde. Dieser Eingriff muss verfassungsrechtlich gerechtfertigt sein. Dafür müssen Inhalt, Zweck und Ausmaß gesetzlich geregelt sein, der Gesetzgeber muss bestmögliche Schutz- und ggf. Strafvorschriften schaffen, um Datenhoheit und Datenintegrität des Einzelnen zu schützen. Schließlich muss die Einführung eines Identifikators den verfassungsrechtlichen Vorgaben der Verhältnismäßigkeit genügen, also ein legitimes Ziel verfolgen, geeignet, erforderlich und angemessen sein.

Bei der zukünftigen Ausgestaltung sind vor diesem Hintergrund insbesondere vier Aspekte relevant: (1) Die Speicherung höchstpersönlicher Daten, insoweit sie heute schon durch das Grundgesetz gedeckt ist, darf nicht erweitert werden. Nicht zu bestreiten ist, dass (2) Daten, die aktuell faktisch vor einer Zusammenführung geschützt sind, durch die Einführung von Identifikatoren grundsätzlich leichter zusammenführbar wären. Zulässig kann die Einführung daher nur dann sein, wenn eine Profilbildung weiterhin effektiv verhindert wird. Dies muss sich auch im Design der Lösung durch entsprechende technische Schutzmechanismen widerspiegeln. (3) Es muss sichergestellt sein, dass ein Datenzugriff bzw. austausch nur mit dem Willen und Einverständnis der Bürger*innen selbst stattfinden kann. (4) Der Zugriff durch staatliche Stellen muss auch in Zukunft auf die notwendigen Daten begrenzt sein, die zur Durchführung eines Verwaltungsaktes benötigt werden.

Im Koalitionsvertrag der Bundesregierung von 2018 sowie in einem Beschluss der Innenministerkonferenz haben sich Bundes- und Länderregierungen auf die Einführung von Identifikatoren als Grundlage für die Registermodernisierung und den registerübergreifenden Datenaustausch verständigt.[11] Mit dem Kabinettsbeschluss zum Registermodernisierungsgesetz

---

[10] Vgl. Martini/Wagner/Wenzel, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer, 2017.

[11] Dieses Ziel ist im Koalitionsvertrag der Bundesregierung festgeschrieben. Zudem gab die Innenministerkonferenz im November 2018 den initialen Anstoß, die technischen und regulatorischen Möglichkeiten für die Registermodernisierung und ein registerübergreifendes Identitätsmanagement zu evaluieren.

wurde das Gesetzgebungsverfahren zur Einführung eines Identifikators im September 2020 auf den Weg gebracht. Im Rahmen des weiteren Gesetzgebungsprozesses gilt es nun, eine Lösung für die Ausgestaltung und Einführung von Identifikatoren unter Beachtung bestehender regulatorischer bzw. gesetzlicher Hürden bei gleichzeitiger Realisierung größtmöglichen technischen Nutzens zu finden.

Als Beitrag zu dieser Abwägung wollen wir im Folgenden auf die verschiedenen Gestaltungsoptionen bei der Einführung von Identifikatoren und ihre Auswirkungen auf die Funktionsweise des eID-Ökosystems und auf die Interoperabilität eingehen. Dabei stellen wir zunächst die unterschiedlichen Stellschrauben für eine konkrete Ausgestaltung von Identifikatoren durch den Staat vor (1). Anschließend werfen wir einen vergleichenden Blick auf die Konfigurierung von Identifikatoren im europäischen Ausland (2). Aus diesen individuellen Umsetzungsbeispielen und ihren Auswirkungen auf die jeweiligen eID-Ökosysteme leiten wir abschließend ein kurzes Fazit und konkrete Handlungsoptionen für eine erfolgreiche Ausgestaltung von Identifikatoren in Deutschland ab (3.3).

1. Stellschrauben zur Ausgestaltung von Identifikatoren in eID-Ökosystemen

Für die konkrete Ausgestaltung von Identifikatoren gibt es verschiedene Stellschrauben, die jeweils einen starken Einfluss auf die Funktionalität eines eID-Ökosystems ausüben. Im Folgenden konzentrieren wir uns auf vier Stellschrauben, die grundlegende Dimensionen von Identifikatoren beschreiben und bei jeder Ausgestaltung von Identifikatoren berücksichtigt werden müssen.

(1) Einheitliche versus bereichsspezifische Identifikatoren: Je nachdem, ob ein Identifikator über alle Bereiche und Register einheitlich verwendet wird oder ob verschiedene bereichsspezifische Identifikatoren nebeneinander existieren, wird zwischen einheitlichen und bereichsspezifischen Identifikatoren unterschieden.

Beispiele für **bereichsspezifische Identifikatoren** sind die deutsche Steueridentifikations-, Sozialversicherungs- oder Krankenversicherungsnummer. Der maßgebliche Vorteil bereichsspezifischer Identifikatoren liegt darin, dass die Zusammenführung personenbezogener Daten aus verschiedenen Quellen erschwert wird.[12] Dadurch wird die Gefahr der staatlichen Profilbildung sowie des Datenmissbrauchs durch potenzielle Innentäter deutlich stärker adressiert als bei einheitlichen Identifikatoren. Um die Verstärkung des Datenschutzes durch bereichsspezifische Identifikatoren realistisch zu bewerten, gilt es jedoch zu beachten, inwiefern andere persönliche Daten registerübergreifend gespeichert werden. Sofern beispielsweise die

[12] Beispielsweise aus staatlichen Registern.

Speicherung persönlicher Daten wie Name, Geburtstag und Geburtsort weiterhin in verschiedenen Registern erfolgt, ist eine Zusammenführung der persönlichen Daten nach wie vor möglich und der zusätzliche Effekt für den Datenschutz eher begrenzt.

Die Nutzung **einheitlicher Identifikatoren** erleichtert die Handhabung für Bürger*innen sowie die schnelle und effiziente Verknüpfung von Informationen innerhalb der Verwaltung erheblich. Die registerübergreifende Verknüpfung personenbezogener Daten mit einem einheitlichen Identifikator macht einen zentralen Mittler für diese Art der Datenverknüpfung obsolet und reduziert somit die Komplexität des Systems erheblich. Zudem vereinfacht ein einheitlicher Identifikator nicht nur den automatisierten Datenaustausch zwischen Behörden, sondern darüber hinaus auch den sektorübergreifenden Austausch von Daten. Müssen privatwirtschaftliche Unternehmen auf personenbezogene Daten eines Kunden zugreifen, genügt die Angabe des einheitlichen Identifikators zur eindeutigen Zuordnung und Abfrage. Den genannten positiven Argumenten ist der Einwand gegenüberzustellen, dass sich die vereinfachte Zusammenführung von persönlichen Daten mittels eines einheitlichen Identifikators nachteilig auf den Datenschutz auswirken kann. Daher müssen adäquate Schutzmaßnahmen etabliert werden.

(2) Öffentliche versus geheime Identifikatoren: Identifikatoren können sich danach unterscheiden, ob sie prinzipiell bekannt oder vollständig geheim sind. Abhängig von diesem Unterscheidungskriterium differenzieren sich Identifikatoren hinsichtlich möglicher Anwendungsfelder.

Öffentliche Identifikatoren stehen generell nicht nur den Behörden zur eindeutigen Verknüpfung von Identität und personenbezogenen Daten zur Verfügung, sondern können auch von der Privatwirtschaft genutzt werden. Der Vorteil öffentlicher Identifikatoren liegt nicht in der eindeutigen Beziehung zwischen Daten und Identität – diese kann auch durch einen geheimen Identifikator hergestellt werden. Der öffentliche Identifikator vereinfacht vielmehr die Verbindung zwischen elektronischer und physischer Identität und macht dadurch eine Vielzahl von Anwendungsfällen leichter umsetzbar. So ermöglicht beispielsweise in Estland der öffentliche Identifikator eine eineindeutige Verknüpfung von E-Signaturen mit den unterschreibenden Personen, die sich durch ihren Personalausweis identifizieren, da dieser Identifikator sowohl in der E-Signatur enthalten als auch auf dem Personalausweis aufgedruckt ist. Zudem vereinfacht ein öffentlicher Identifikator die Zuweisung von Rechten und Vollmachten an Dritte. In der estnischen elektronischen Patientenakte kann beispielsweise durch die Angabe von Vor- und Nachnamen sowie des öffentlichen Identifikators in Kombination mit einer E-Signatur die Berechtigung zur Abholung verschreibungspflichtiger Medikamente an Dritte erteilt werden. Durch die Verwendung des öffentlichen Identifikators ist eine einfache, eineindeutige Zuweisung

dieser Vollmacht möglich.[13] Im österreichischen System können Rollen und Rechte zwar ebenfalls mithilfe geheimer Identifikatoren vergeben werden, dies gestaltet sich jedoch komplexer und erfordert die Eingabe mehrerer Basisdaten, um die Vertretungsperson eindeutig zu benennen und einen Vertretungseintrag zu erstellen.

Ein weiterer häufiger Anwendungsfall öffentlicher Identifikatoren ist die Verwendung als Benutzername für die E-Authentifizierung. Sowohl für die dänische NemID als auch für die estnische Smart-ID wird weitestgehend der öffentliche Identifikator als Nutzername verwendet. Damit tragen öffentliche Identifikatoren dazu bei, die Nutzbarkeit und Einfachheit des eID-Ökosystems zu stärken.

Geheime Identifikatoren haben den Vorteil, dass sie – zusätzlich zur Segmentierung in verschiedene Bereiche – die Verknüpfung von personenbezogenen Daten mit einer bestimmten Person weiter erschweren. Geheime Identifikatoren werden überwiegend für den innerbehördlichen Datenaustausch verwendet. Im Gegensatz zu einem öffentlichen Identifikator erschwert die Geheimhaltung des Identifikators jedoch die eineindeutige Verknüpfung zwischen physischer und elektronischer Identität. Dies kann negative Implikationen für die Datensparsamkeit von Registern und insbesondere Fachanwendungen haben[14], wenn für die Identifikation einer Person bei persönlichem Erscheinen weiterhin persönliche Daten vorgehalten werden. Zudem lässt sich die eineindeutige Verknüpfung von physischer und elektronischer Identität anhand eines öffentlichen Identifikators deutlich einfacher darstellen.

Geheimen Identifikatoren bleiben darüber hinaus einige Anwendungsfälle, die im Kontext öffentlicher Identifikatoren soeben skizziert wurden und unter Umständen zuträglich für die Akzeptanz und Nutzung des eID-Ökosystems durch die breite Masse der Bevölkerung wären, verwehrt.

(3) Lebenslange versus wechselnde Identifikatoren: Ein weiteres grundlegendes Unterscheidungskriterium von Identifikatoren bezieht sich auf die Dauer ihrer Gültigkeit – konkret darauf, ob sie einmalig für das ganze Leben vergeben werden oder sich im Laufe des Lebens verändern.

Ein in Deutschland mit **lebenslanger** Geltung vergebener **Identifikator** ist beispielsweise die steuerliche Identifikationsnummer. In Ländern wie Estland und Dänemark sind die Identifikatoren von Geburt an ein wichtiger Bestandteil im Umgang der Bürger*innen mit

---

[13] Das gleiche Prinzip wird in einer Vielzahl von Anwendungsfällen genutzt, wie z. B. bei der Erteilung des Zugriffs auf Bankkonten, der Benennung von berechtigten Fahrer*innen für Dienstwagen, der Übertragung des Besitzes eines Fahrzeugs oder bei der Bestellung von vertretungsberechtigten Personen für Unternehmen.

[14] Demnach ist davon auszugehen, dass geheime Identifikatoren auch die Umsetzung des Once-Only-Prinzips erschweren.

Behörden- und Unternehmensdienstleistungen. Lebenslange Identifikatoren verringern die Komplexität und steigern die Einfachheit der Benutzung erheblich.

Von **wechselnden Identifikatoren** spricht man, wenn diese beispielsweise nach Statusänderungen oder für jedes Verfahren neu vergeben werden. Beispiele sind Immatrikulations-, Verfahrensreferenz- oder Versichertennummern. Bis zur Einführung der elektronischen Gesundheitskarte erhielt man in Deutschland bei einem Wechsel der Krankenkasse eine vollständig neue Versichertennummer. Heute ist die Versichertennummer eine Kombination eines unveränderlichen und eines veränderlichen Teils, wobei Letzterer u. a. die Kassenzugehörigkeit enthält.[15] Auch bei jeder Beantragung eines neuen Personalausweises wird in Deutschland eine neue Seriennummer für das neu ausgestellte Ausweisdokument vergeben. Wechselnde Identifikatoren haben den Vorteil, dass sie ein zusätzliches Maß an Vertrauenswürdigkeit bieten, indem sie die Zusammenführung von persönlichen Daten erschweren.

(4) Zufällig generierte Identifikatoren versus Identifikatoren mit persönlichen Informationen: Sowohl bei den beinhalteten Informationen als auch bei der Anordnung der Stellen eines Identifikators gibt es unterschiedliche Gestaltungsmöglichkeiten. Ein Identifikator kann entweder zufällig generiert bzw. pseudonymisiert werden, beispielsweise in Form einer Nummernfolge, oder er kann persönliche Informationen beinhalten, wie etwa das Geburtsdatum. Ein Mittelweg im Kontext dieser Gestaltungsdimension sind Identifikatoren mit einer Codierung persönlicher Informationen, welche aber nur mithilfe eines (staatlichen) Schlüssels zurückgerechnet werden können. In Deutschland ist man darauf bedacht, im Rahmen der Einführung eines Identifikators die Eingriffstiefe in die Grundrechte möglichst gering zu halten. Die Intensität des Eingriffs ist dabei umso geringer, je weniger Persönlichkeitsrelevanz der Identifikator enthält.[16] Vor diesem Hintergrund wird es in Deutschland voraussichtlich keinen Identifikator geben, der die Möglichkeit bietet, auf persönliche Informationen rückzuschließen. Aus Gründen der Vollständigkeit wird diese Unterscheidung hier dennoch aufgeführt.

Neben den dargestellten vier allgemeinen Stellschrauben zur Gestaltung von Identifikatoren gilt es hinsichtlich der grundlegenden Infrastruktur, des Datenaustauschs und der Umsetzung drei zusätzliche Aspekte zu beachten. Auf diese gehen wir im Folgenden ein.

---

[15] Die Krankenversicherungsnummer hat zwischen 20 und 30 Stellen. Der unveränderliche Teil der Nummer ist auf der Karte physisch aufgedruckt, elektronisch ist im System aber eine längere Nummer hinterlegt, die u. a. auch die Ziffern der Kassenzugehörigkeit enthält. Eine Anpassung des veränderlichen Teils bei einem Kassenwechsel findet daher nur elektronisch im System statt.

[16] Vgl. Zwischenbericht für die Innenministerkonferenz (4. – 6. Dezember 2019): Registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung.

(a) Errichtung einer bundesweiten Infrastruktur für den Identifikator

Die Einführung eines Identifikators und die Sicherstellung einer effizienten registerübergreifenden Datenübermittlung funktionieren nur auf Basis einer adäquaten Infrastruktur. Im Zwischenbericht für die Innenministerkonferenz (IMK) vom Dezember 2019 werden mehrere Optionen für den Aufbau einer solchen Infrastruktur dargestellt.

Grundsätzlich streben Bund und Länder an, bestehende Infrastrukturen zu nutzen und auszubauen. Für das Identitätsmanagement der deutschen Registerlandschaft kommen gemäß IMK drei Ausgestaltungsmöglichkeiten in Betracht: die Nutzung der Steuer-ID-Datenbank mit der Steuer-ID beim Bundeszentralamt für Steuern (BZSt), die Verwendung der 15 Landesmelderegister sowie des Meldeportals in NRW oder der Aufbau eines neuen Identitätenregisters in der Innenverwaltung. Eine Entscheidung für den Neuaufbau ist dabei sehr unwahrscheinlich, da dieser mit einem enormen Kostenaufwand verbunden wäre. So benötigte das BZSt – unter Einberechnung aller Prozesse inklusive Qualitätssicherung – für den Aufbau der Infrastruktur vier bis sechs Jahre.[17] Das BZSt verfügt über eine bestehende Infrastruktur mit einer Steuer-ID-Datenbank, die alle Daten zur eindeutigen Identifikation der Bürger*innen bereits enthält und darüber hinaus in ständigem Austausch mit Registern anderer Behörden (z. B. Melderegister) steht. Mit Blick auf die Anforderungen der IMK für ein Identitätsmanagement in der Innenverwaltung erfüllt die Infrastruktur des BZSt bereits einen Großteil der Vorgaben.

Zur Sicherstellung und Optimierung der Interoperabilität hat die IMK beschlossen, auf bereits existierenden Standards aufzubauen und diese fortzuentwickeln. Entsprechend sollen etwa einheitliche Standards zu Datenhaltung und -austausch registerübergreifend weiterentwickelt und durchgesetzt werden.

(b) Erfordernisse an die Zustimmung zum Datenaustausch – explizite Zustimmung an separater Stelle (Konsensmodul) vs. Zustimmung im Antragsprozess

Um den Bürger*innen innerhalb des an das eID-Ökosystem angrenzenden Interoperabilitätssystems Kontrolle über ihre Daten zu verschaffen, ist es notwendig, für eine klare Handhabung bezüglich der Zustimmungsmethode zum Datenaustausch zu sorgen. Dabei können zwei verschiedene Ansätze herangezogen werden, die sich hinsichtlich des Zustimmungsprozesses unterscheiden. Zum einen kann ein Zustimmungsprozess über ein Konsensmodul an separater Stelle erfolgen. Existiert beispielsweise die Möglichkeit eines automatisierten Datenaustauschs, der allerdings nicht gesetzlich vorgeschrieben ist, können die Bürger*innen ihre explizite Zustimmung dazu geben. Mithilfe eines zentralen Moduls kann auch eine Vielzahl von Einwilligungen transparent und im Sinne der Datensouveränität von den

[17] Vgl. Zwischenbericht für die Innenministerkonferenz (4. – 6. Dezember 2019): Registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung.

Bürger*innen verwaltet werden. Zum anderen kann die Zustimmung zum Datenaustausch direkt in den Antragsprozess integriert werden. Das hat den Vorzug, dass die Einwilligung nicht an separater Stelle stattfinden muss, sondern der Einfachheit halber über einen Klick erfolgt. Eine zentrale Stelle zur Einsichtnahme in die erteilten Einwilligungen gibt es in diesem Fall allerdings nicht.

(c) Art der Einführung – einheitlicher Rollout vs. anlassbezogene Eintragung in Fachregister

Eine der größten Herausforderungen bei der Einführung von Identifikatoren besteht darin, diese an sämtlichen relevanten Stellen nachzupflegen. Besonders im deutschen Registersystem sind personenbezogene Daten sehr fragmentiert in verschiedenen Registern abgespeichert. Zudem unterscheiden die Daten sich häufig in ihrer Aktualität und Validität aufgrund inkonsistenter Methoden der Speicherung.

Ein denkbarer Ansatz zur Einführung eines Identifikators ist ein vollständiger Rollout über alle oder mehrere Register hinweg. In einem groß angelegten Rollout würden die neuen Identifikatoren in allen oder bestimmten Registern vollständig nachgepflegt. Diese Methode würde jedoch einen enormen Ressourceneinsatz erfordern. Es könnte Jahre, vielleicht sogar Jahrzehnte dauern, bis alle Angleichungs- und Verknüpfungsprozesse abgeschlossen wären. Der damit einhergehende Aufwand an Kosten und Ressourcen wäre nur schwer überschaubar. Als Referenzwert kann der Aufbau der Steuer-ID-Datenbank dienen, für den das BZSt vier bis sechs Jahre benötigte.[18]

Ein zweiter möglicher Ansatz zur Einführung eines Identifikators ist die Methode der anlassbezogenen Eintragung in die Fachregister. In diesem Fall finden die Aktualisierung und Verknüpfung der Daten nur dann statt, wenn eine Person mit einem Register in Kontakt tritt. Diese Vorgehensweise bietet den Vorteil einer erheblichen Einsparung von Kosten und Ressourcen. Ein Nachteil könnte sein, dass der eigentlich automatisierte Datenaustausch beim Erstkontakt unterbrochen wird und manuell bearbeitet werden muss.

Im folgenden Abschnitt geben wir vor dem Hintergrund der möglichen Stellschrauben der Ausgestaltung von Identifikatoren einen Überblick über Identifikatorenmodelle in anderen europäischen Ländern. Im Fokus stehen dabei die Staaten Estland und Österreich, deren konträre Modelle hinsichtlich ihrer Potenziale und Risiken beleuchtet werden.

[18] Vgl. Zwischenbericht für die Innenministerkonferenz (4. – 6. Dezember 2019): Registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung.

2. Blick ins europäische Ausland: Ausgestaltung von Kennziffern und Auswirkungen auf das jeweilige eID-Ökosystem

Für die Debatte über die Gestaltung von Identifikatoren in Deutschland bieten die verschiedenen Identifikatorenmodelle im europäischen Ausland wertvolle Lehren und Impulse. In diesem Abschnitt werden wir ausgewählte europäische eID-Ökosysteme entlang der Stellschrauben für Identifikatoren darstellen. Dabei wird jeweils beschrieben, wie sich die Stellschrauben auf das jeweilige eID-Ökosystem entlang der aufgestellten qualitativen Bewertungskriterien Nutzbarkeit, Einfachheit und Vertrauenswürdigkeit auswirken. Als oft genannte – und dabei in ihrem Wesen grundverschiedene – Beispiele guter Praxis im Bereich eID stehen hier insbesondere das estnische (1) und das österreichische Modell (2) im Fokus. Diese sind jeweils nicht als mögliche 1:1-Vorbilder für eine Umsetzung in Deutschland zu verstehen, sondern vielmehr als entgegengesetzte Typen in einem Spektrum verschiedener Ausgestaltungsmöglichkeiten, die so oder in abgewandelter Form auch in anderen Ländern entwickelt wurden.

Die Nutzung eines Identifikators zur eindeutigen und effizienten Übermittlung von Daten im Rahmen von Behördenprozessen ist in den Staaten der EU weit verbreitet. Lediglich 5 der 27 Mitgliedstaaten haben keinen Identifikator eingeführt – dazu zählt auch Deutschland. Einige Identifikatoren beinhalten personenbezogene Daten, wie beispielweise das Geburtsdatum, andere Identifikatoren bestehen aus zufällig generierten Zahlenfolgen. Unter den 22 Identifikatorenmodellen ist das österreichische das einzige in Europa, das eine geheime Stammzahl in Verbindung mit geheimen bereichsspezifischen Identifikatoren nutzt. Damit nimmt das österreichische System eine absolute Außenseiterrolle im Vergleich der Identifikatorenmodelle der EU-Mitgliedstaaten ein.

EU 27	Identifikator	Name	Einheitlich vs. bereichsspezifisch	Öffentlich vs. geheim	Lebenslang vs. wechselnd	Datenschutz-kritischer Identifikator	Auf Ausweismedium enthalten
Belgien	Ja	Numéro de registre national / Rijksregisternummer	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Bulgarien	Ja	Edinen grazhdanski nomer	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Dänemark	Ja	CPR-nummer	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Deutschland	Nein						
Estland	Ja	Isikukood	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Finnland	Ja	HETU - Henkilötunnus	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Frankreich	Ja	NIR - Numéro d'inscription au répertoire	Einheitlich	Öffentlich	Lebenslang	Ja	Sozialversicherungs-ausweis
Griechenland	Nein						
Irland	Ja	Personal Public Service Number	Einheitlich	Öffentlich	Lebenslang	Nein	Public Service Card
Italien	Ja	Codice fiscale	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Kroatien	Ja	OIB - Osobni identifikacijski broj	Einheitlich	Öffentlich	Lebenslang	Nein	Personalausweis
Lettland	Ja	Personas kods	Einheitlich	Öffentlich	Lebenslang	Nein*	Personalausweis
Litauen	Ja	Asmens kodas	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Luxemburg	Ja	-	Einheitlich	Öffentlich	Lebenslang	Ja	Sozialversicherungs-ausweis
Malta	Ja	-	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Niederlande	Ja	BSN - Burgerservicenummer	Einheitlich	Öffentlich	Lebenslang	Nein	Personalausweis
Österreich	Ja	bPK - Bereichsspezifisches Personenkennzeichen und Stammzahl	Bereichsspezifisch	Geheim	Lebenslang	Nein	Nein
Polen	Ja	PESEL - Powszechny Elektroniczny System Ewidencji Ludności	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Portugal	Nein						
Rumänien	Ja	Cod Numeric Personal	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Schweden	Ja	Personnummer	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Slowakei	Ja	Rodné číslo	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Slowenien	Ja	Enotna matična številka občana	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Spanien	Ja	Código de identificación fiscal	Einheitlich	Öffentlich	Lebenslang	Nein	Personalausweis
Tschechien	Ja	Rodné číslo	Einheitlich	Öffentlich	Lebenslang	Ja	Personalausweis
Ungarn	Nein						
Zypern	Nein						

*Alle nach 2017 vergebenen Kennziffern enthalten keine Geburtsdaten mehr.

Tabelle 1: Übersicht nationaler Identifikatoren der EU 27

Die Modelle der 22 Staaten unterscheiden sich hinsichtlich der untersuchten Stellschrauben kaum. Diese Erkenntnis verdeutlicht die Notwendigkeit, die Beweggründe, Chancen und Risiken der zwei unterschiedlichen Ansätze zu verstehen und herauszuarbeiten. Als Repräsentant für Systeme mit einem einheitlichen, nicht-geheimen Identifikator wird Estland gewählt, da dieses Land sich zusätzlich durch einen hohen Grad an Datenaustausch über sein Interoperabilitätssystem „X-Road“ auszeichnet.

1. Das estnische Modell

Das estnische Modell weist in seinen Grundzügen große Ähnlichkeit mit der Ausgestaltung von Identifikatoren u. a. in Dänemark, Schweden und Belgien auf. Es ist geprägt durch einen einheitlichen, öffentlichen, lebenslangen Identifikator sowie umfassende Transparenz für Bürger*innen über die Nutzung persönlicher Daten im Rahmen des innerbehördlichen und sektorübergreifenden Datenaustauschs.

Der estnische Identifikator „Isikukood“ ist 1989 aus einem Pilotprojekt der damaligen UdSSR hervorgegangen. Er besteht aus einer **öffentlichen Zahlenkombination**, in der **persönliche Informationen**, wie Geschlecht und Geburtsdatum der Person, enthalten sind. Der Isikukood wird im Normalfall innerhalb weniger Stunden nach der Geburt infolge einer Meldung des Krankenhauses an das Bevölkerungsregister erstellt und bleibt **lebenslang unverändert**. Aufgrund seiner **einheitlichen Gestaltung** und des **Verzichts auf Geheimhaltung** ist der Isikukood sowohl im öffentlichen als auch im privaten Sektor einfach nutzbar und bietet eine Vielzahl von Anwendungsmöglichkeiten.

Wie eingangs in Abschnitt 1 beschrieben, begünstigt die öffentliche Verwendbarkeit des Isikukood die einfache Zuweisung von Rollen und Rechten. Für bestimmte elektronische Identifizierungsmittel dient der Isikukood als Nutzername bei der E-Authentifizierung für E-Services der öffentlichen Verwaltung und im Privatsektor. Im privaten Sektor wird der Identifikator darüber hinaus beispielsweise im Rahmen von Loyalitätsprogrammen eingesetzt.

Zudem ist er auf dem estnischen Personalausweis aufgedruckt und in den darauf enthaltenen elektronischen Zertifikaten für E-Authentifizierung und E-Signatur gespeichert. So ist einerseits eine einfache Verknüpfung elektronischer und physischer Identitäten möglich. Andererseits wird dadurch das Record-Matching bei E-Authentifizierung und E-Signatur zwischen Zertifikatsdaten und den entsprechenden personenbezogenen Daten des Online-Diensteanbieters vereinfacht.

„Isikukood“ als Grundlage für einfache Interoperabilität

Durch die frühe Einführung des Isikukood in den späten 1980er Jahren konnte dieser bei der Erstellung von elektronischen Registern von Anfang an miteinbezogen werden. Die Qualität der

Registerdaten in Estland ist entsprechend hoch. Seit etwa 30 Jahren werden die Daten mit einem Identifikator verknüpft und gepflegt. Damit besaß Estland einen entscheidenden Vorteil gegenüber anderen Staaten, die Identifikatoren in bestehenden elektronischen Registern nachpflegen mussten.

Seit knapp 20 Jahren arbeitet Estland zudem am Aufbau des einheitlichen Interoperabilitätssystems X-Road[19], das für den elektronischen Datenaustausch zwischen Behörden und mit dem Privatsektor genutzt wird. Die flächendeckende Verwendung des Isikukood in der estnischen Registerlandschaft erweist sich dabei als signifikanter Vorteil, denn dadurch lässt sich beim elektronischen Datenaustausch eine äußerst geringe Fehlerquote sicherstellen. Der automatische Datenaustausch über die X-Road hat seit ihrer Einführung im Jahr 2001 kontinuierlich zugenommen und erreichte im Jahr 2019 mit mehr als 1,3 Milliarden Anfragen seinen bisherigen Höchststand. Bezogen auf die Einwohnerzahl sind dies mehr als 1.000 Anfragen pro Person im Jahr, wobei nur ein Teil dieser Anfragen personenbezogene Daten betrifft. Aufgrund der Entwicklung immer weiterer Verfahren, welche die Möglichkeit des automatischen Datenaustauschs über die X-Road nutzen, ist davon auszugehen, dass die Zahl der Transaktionen weiterhin steigen wird. Beispielsweise fokussiert sich Estland aktuell stark auf die Entwicklung antragsloser Verfahren, die allein durch einen automatisierten elektronischen Datenaustausch ermöglicht werden.

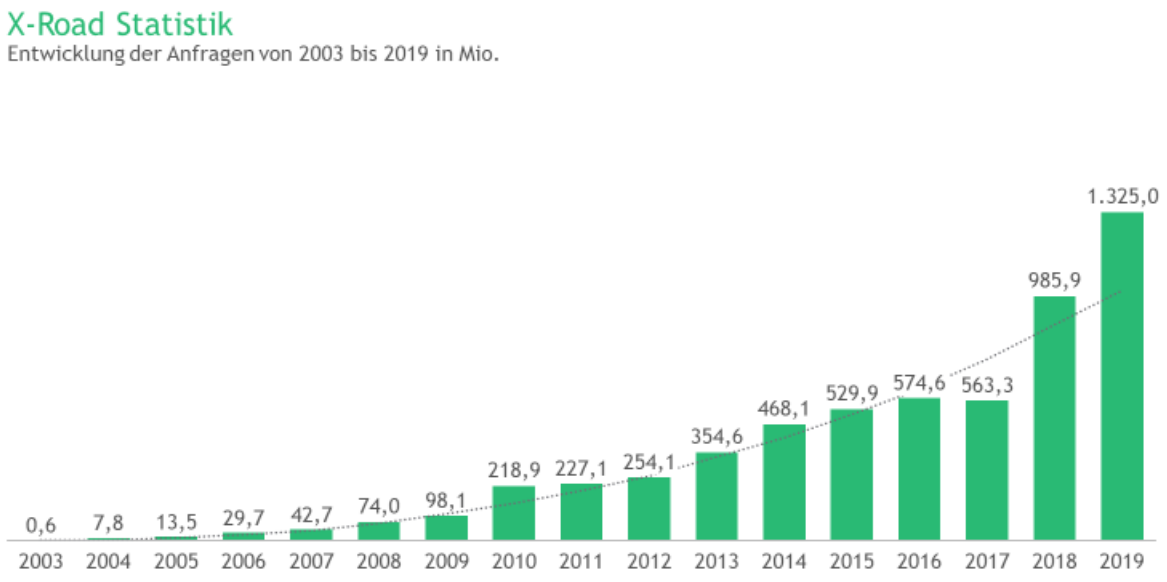


Abbildung 4: Entwicklung der X-Road-Anfragen von 2003 bis 2019[20]

---

[19] Die X-Road wurde in Estland entwickelt und ist ein System zum sicheren Datenaustausch zwischen Institutionen. Im Laufe der Zeit wurde dieses System in mittlerweile 13 Nationen implementiert.

[20] Vgl. X-TEE (2020): Factsheets.

Auch für den grenzüberschreitenden Datenaustausch zwischen Behörden, beispielsweise im Bereich des Steuerwesens, bilden das X-Road-System und der Isikukood eine wichtige Grundlage. Finnland nutzt die X-Road ebenfalls und hat sie mit der estnischen X-Road-Instanz verbunden. Das ermöglicht es mittlerweile, z. B. elektronische Arzneimittelrezepte aus einem Land in dem anderen Land einzulösen.

Ein weiterer Nutzen, der aus dem hohen Grad der Vernetzung der estnischen Verwaltung und Unternehmen über die X-Road resultiert, liegt in den Erkenntnissen, die aus den Datenflüssen gewonnen werden können.[21] Somit kann ein entwickeltes Interoperabilitätssystem auch als Grundlage für evidenzbasierte Politikgestaltung dienen.

Ursprünglich wurde die X-Road als Plattform für den öffentlichen Sektor entwickelt. Inzwischen steigen Nutzung und Nutzbarkeit für die Privatwirtschaft kontinuierlich an. Dies geht in großen Teilen auf Anwendungsfälle zurück, bei denen der Staat Unternehmen verpflichtet, Daten elektronisch zu übertragen, insbesondere in Anwendungsfällen mit Bezug auf Finanzen und Steuern. Zudem wurde in der estnischen Digitalen Agenda 2020 aus dem Jahr 2013 das Ziel verankert, den Zugang zur X-Road für Unternehmen zu vereinfachen, damit auch diese den automatischen Datenaustausch nutzen können, um die Effizienz ihrer Prozesse zu steigern. Obwohl die Kosten für die Registrierung als X-Road-Mitglied derzeit noch relativ hoch sind, übertrifft die Zahl der nichtstaatlichen Organisationen (einschließlich Unternehmen) unter den Mitgliedern der X-Road inzwischen die Zahl der Behörden.

[21] Beispielsweise kann die Wirtschaftskraft Estlands anhand von Daten, die über die X-Road fließen, nahezu in Echtzeit mit hoher Genauigkeit gemessen werden.

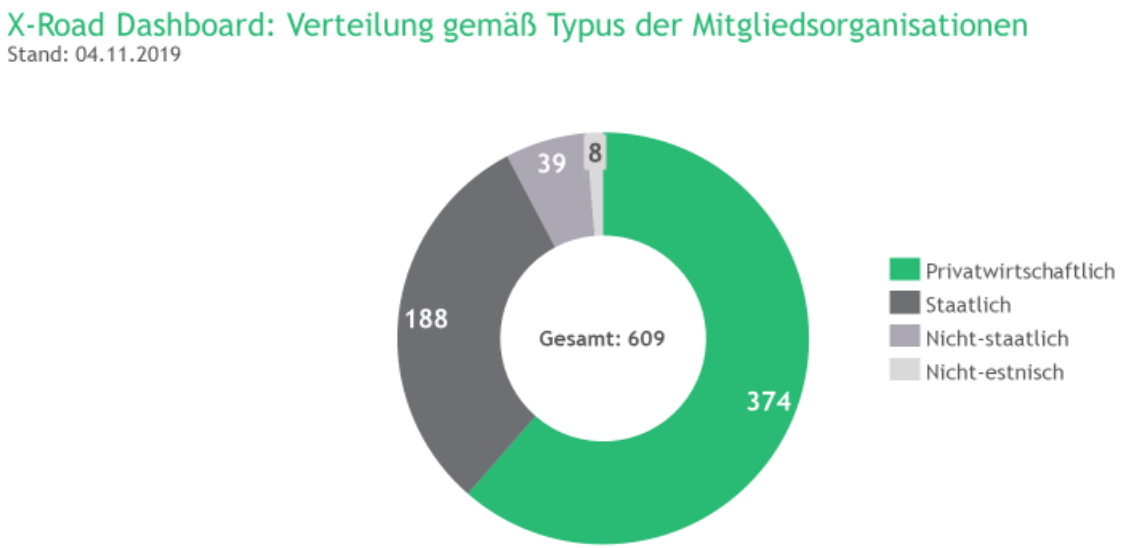


Abbildung 5: X-Road-Mitgliedsorganisationen nach Typus[22]

So profitieren beispielsweise Banken von einer direkten Schnittstelle mit dem Melderegister, um die Daten ihrer Kunden auf Grundlage des Isikukood validieren zu können. Studierende, die einen Studienkredit beantragen, müssen keine Immatrikulationsbescheinigung mehr vorlegen, da die Bank über die X-Road den Studierendenstatus bei der entsprechenden Behörde abfragen kann.

Als weiteren Schritt zur Einbindung der Privatwirtschaft entwickelt Estland derzeit ein Konsensmodul, das direkt an die X-Road angeschlossen ist und zu dem Bürger*innen über das Bürgerkonto[23] Zugang haben. Konkret soll damit Unternehmen die Möglichkeit gegeben werden, personenbezogene Daten der Behörden nach expliziter Zustimmung der Bürger*innen zu nutzen, auch wenn im konkreten Fall keine spezifische gesetzliche Grundlage für den Datenaustausch existiert. Mit dem Konsensmodul der X-Road soll es für Unternehmen zukünftig möglich sein, auf Basis ausdrücklicher Zustimmung auf persönliche Daten der Bürger*innen zuzugreifen. Mit dem Konsensmodul kann dies auch ohne explizite gesetzliche Grundlage für einen spezifischen Anwendungsfall geschehen und ermöglicht es Unternehmen so maßgeschneiderte Dienstleistungen für Bürger*innen anzubieten, regulatorische Hürden zu überwinden und das Potenzial ihres Geschäftsmodells vollständig auszuschöpfen. So will beispielsweise ein estnisches Start-up Bürger*innen den Service anbieten, ihre Impfdaten zu analysieren und sie automatisch

[22] Vgl. Information System Authority (RIA) (2019).

[23] Alle estnischen Bürger*innen haben über das zentrale E-Government-Portal, eesti.ee, Zugang zu ihren persönlichen Daten, ihrem Postfach, verschiedenen E-Services sowie einem „Data Tracker“, über den der behördenübergreifende Zugriff auf persönliche Daten nachvollzogen kann.

an Impfungen zu erinnern. Mit einer Integration zur elektronischen Patientenakte über die X-Road und der expliziten Zustimmung über das Konsensmodul wäre das Start-up in der Lage, auf die Impfdaten der jeweiligen Person zuzugreifen und den Service schneller und nutzerfreundlicher zu gestalten.

Bewertung des estnischen Modells

(1) Nutzbarkeit

Die hohe Nutzbarkeit des estnischen Isikukood wird insbesondere durch seine simple Ausgestaltung gefördert. Die Nichtgeheimhaltung in Kombination mit Einheitlichkeit und lebenslanger Nutzung erhöht die Anzahl möglicher Anwendungsfälle des Identifikators bzw. vereinfacht deren Umsetzung, insbesondere im Vergleich zu geheimen, bereichsspezifischen und wechselnden Identifikatoren. Zudem steigert diese Ausgestaltung die Nutzbarkeit des Isikukood durch die Privatwirtschaft und erleichtert wiederum deren Anbindung an das estnische Interoperabilitätssystem. Dadurch werden eine sektorübergreifende Nutzung der X-Road und die Realisierung von Effizienzpotenzialen der Interoperabilität über die Verwaltung hinaus vereinfacht.

(2) Einfachheit

Die simple Ausgestaltung des Isikukood als einheitlicher, nicht-geheimer Identifikator erhöht die Einfachheit der Nutzung in einer Vielzahl von Anwendungsfällen für Bürger*innen, Unternehmen und die Verwaltung. Entscheidender für den langfristigen Erfolg staatlicher Digitalisierungsbemühungen sowie die Zukunftsfähigkeit des Staates könnte jedoch sein, dass die einfache Ausgestaltung des Identifikators auch die Komplexität der Umsetzung von digitalen Services und Fachanwendungen dauerhaft minimiert.[24]

(3) Vertrauenswürdigkeit

Die Verwendung einheitlicher, nicht-geheimer und lebenslang gültiger Identifikatoren vereinfacht die Zusammenführung von persönlichen Daten. Das beeinträchtigt die

[24] Experteninterviews legen den Schluss nahe, dass Estland in der Umsetzung von Fachanwendungen stark von der Simplizität seines Systems profitiert, während die Umsetzung von Fachanwendungen in Österreich aufgrund der dortigen Ausgestaltung der Identifikatoren deutlich komplexer ist. Estland hat sich bewusst dafür entschieden, die Komplexität seines eID-Ökosystems möglichst gering zu halten, um die Entwicklungskosten zu minimieren und die Zukunftsfähigkeit des Systems zu maximieren. Diese strategische Herangehensweise basiert auf dem sogenannten KISS-Prinzip („Keep it short and simple“).

Vertrauenswürdigkeit des estnischen Modells. Problematisch im Hinblick auf den Grundsatz der Datenminimierung ist zudem die Beinhaltung persönlicher Informationen im Isikukood.[25]

Trotz dieser Bedenken bietet das estnische Modell durch die Ausgestaltung des Interoperabilitätssystems weitgehende Transparenz über Zugriffe auf persönliche Daten, wie sie so aktuell weder in Deutschland noch in Österreich möglich ist. Jede Übermittlung personenbezogener Daten über die X-Road wird dokumentiert und kann von der betroffenen Person in einem Datenschutzcockpit eingesehen werden.[26] Die Esten bezeichnen dies auch als „Little Brother"-Ansatz.

Weiterhin dürfen Datenabfragen in der Regel nur erfolgen, wenn eine Person den Prozess durch ein Anliegen auslöst. Unautorisierte Zugriffe auf Daten können auf diese Weise schnell und unkompliziert aufgedeckt und entsprechend geahndet werden. Mit der Rückverfolgbarkeit von Datenzugriffen ermöglicht Estland einen so hohen Grad an Transparenz wie kaum ein anderes Land in Europa. Nach Experteneinschätzung sind es diese transparenten Prozesse, welche die Grundlage für die Vertrauensbildung seitens der Bürger*innen legen.[27] [28]

Im Hinblick auf die Sicherheit persönlicher Daten geht die hohe Transparenz in Estland jedoch nicht mit einem vergleichbaren Maß an Kontrollmöglichkeiten für Bürger*innen einher. Die Möglichkeit zur nachträglichen Einsicht und Ahndung verhindert nicht grundsätzlich unrechtmäßige bzw. unautorisierte Datenzugriffe, was die Kontrolle der Bürger*innen über ihre persönlichen Daten schwächt (Datensouveränität). Vor dem Hintergrund der kulturell und historisch gewachsenen hohen Sicherheitsbedenken deutscher Bürger*innen in Bezug auf den staatlichen Zugriff auf bzw. die Speicherung ihrer Daten ist dieser Aspekt kritisch zu beurteilen.

---

[25] Vgl. Martini/Wenzel (2017): Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern.

[26] Eine Ausnahme bilden polizeiliche oder geheimdienstliche Ermittlungen. Zwar wird in solchen Fällen der Zugriff dokumentiert, für die Dauer des Verfahrens ist dieser aber für die betroffene Person nicht sichtbar. Nach dem Verfahren kann die vollständige Historie eingesehen werden. Über das in das Bürgerkonto integrierte Datenschutzcockpit sind aktuell nur die Zugriffe auf persönliche Daten aus vier Registern einsehbar. Datenzugriffe in anderen Registern können von den Bürgern bei der zuständigen Datenschutzstelle erfragt werden. Zudem gilt dieses Prinzip auch für die elektronische Patientenakte, in der eingesehen werden kann, welche Personen auf die eigenen medizinischen Daten zugegriffen haben.

[27] Angabe aus Experteninterviews des Projektteams.

[28] Ein Blick nach Dänemark zeigt, dass auch hier eine vollständige Transparenz der Nutzung personenbezogener Daten gewährleistet wird. Über das Bürgerportal „borger.dk" lassen sich nicht nur alle Zugriffe auf die eigenen Daten nachvollziehen, sondern im Sinne der Datensouveränität auch festlegen, welche Institutionen für den Zugriff auf die persönlichen Daten autorisiert sein sollen.

2. Das österreichische Modell

Im Gegensatz zur Verwendung einheitlicher, nicht-geheimer Identifikatoren im estnischen Modell hat sich Österreich für ein komplexeres, in Europa einzigartiges System entschieden, um ein Höchstmaß an Datenschutz zu gewährleisten. Mit dem österreichischen E-Government-Gesetz von 2004 wurden **geheime, bereichsspezifische Personenkennzeichen** (bPK) für 35 verschiedene Verfahrensbereiche eingeführt, die über eine nicht umkehrbare Ableitung aus der **geheimen, zentralen Stammzahl** einer natürlichen Person gebildet werden. Sowohl die geheime Stammzahl einer Person als auch die bPK bleiben prinzipiell **lebenslänglich** bestehen. Alle Identifikatoren enthalten **keine personenbezogenen Daten**. Hauptgrund für diese Ausgestaltung des Identifikatorensystems waren datenschutzrechtliche Bedenken, aus denen das Ziel resultierte, die unrechtmäßige Zusammenführung von Daten aus verschiedenen Verfahrensbereichen zu erschweren. Da unterschiedliche Bereiche verschiedene Identifikatoren für personenbezogene Daten verwenden, können diese nicht so einfach zusammengeführt werden, wie es bei der Nutzung einheitlicher Identifikatoren der Fall wäre.

Für die Erstellung und Verwaltung der Identifikatoren sowie die Ermöglichung der Zusammenführung von Daten in berechtigten Fällen wurde eine zentrale Stammzahlenregisterbehörde geschaffen, die mittlerweile dem Bundesministerium für Digitalisierung und Wirtschaftsstandort angehört.

Die Stammzahlenregisterbehörde in Österreich erfüllt als **Dreh- und Angelpunkt** mehrere Funktionen: Sie nimmt u. a. (1) die Ableitung und Führung der Stammzahl aus dem zentralen Melderegister und dem Ergänzungsregister vor. Sie leitet (2) aus der geheimen Stammzahl die bPK ab und stattet die verschiedenen bereichsspezifischen Register mit bPK aus. Sie koordiniert (3) das „Record-Matching“, d. h. die zweifelsfreie Zuordnung von Registereinträgen zu natürlichen Personen. Die Stammzahlenregisterbehörde agiert (4) als zentrale Vermittlungsstelle für behördliche Datenabfragen, bei welchen (wiederum über die Stammzahl) Informationen verschiedener Behörden mit jeweils eigenen bPK verknüpft werden müssen.[29] Zudem verwaltet sie (5) das Register für Online-Vollmachten und betreut den Online-Vollmachten-Service. Bei einer Anmeldung durch eine Vertretungsperson überprüft die Behörde alle zur Verfügung stehenden Vertretungsvollmachten aus den bereichsspezifischen Registern. Ihre Funktionen erfüllt die Stammzahlenregisterbehörde somit zum einen bei der initialen Ausstattung mit, aber auch bei der

---

[29] Die bPK werden auf Basis der Stammzahl und des entsprechenden Verfahrensbereichs mit einem nicht umkehrbaren Verfahren berechnet. Bei bereichsübergreifenden Datenaustauschverfahren auf Basis gesetzlicher Grundlagen werden Datenkonsumenten mit verschlüsselten bereichsspezifischen Personenkennzeichen (vbPK) der Bereiche, aus denen sie Daten benötigen, ausgestattet. Dazu muss ein Antrag bei der Stammzahlenregisterbehörde gestellt werden, die in der Folge auch für die Ausstattung mit vbPK zuständig ist. Diese werden verschlüsselt an den Zielbereich übermittelt und können nur von Behörden in diesem Bereich entschlüsselt und der entsprechenden Person zugeordnet werden.

unter Umständen erforderlichen Neuberechnung von bPK (z. B. bei Datenabfragen ohne Beteiligung der Bürger*innen auf Basis gesetzlicher Grundlagen).

Zudem ist die Stammzahl verschlüsselt auf den staatlichen elektronischen Identifizierungsmitteln (Bürgerkarte und Handysignatur) gespeichert. Mithilfe der Bürgerkartenumgebung – der für die Verwendung der Bürgerkarte notwendigen Software – können bPK direkt durch die Bürger*innen gebildet und zur E-Authentifizierung bzw. E-Signatur im jeweiligen Bereich genutzt werden.

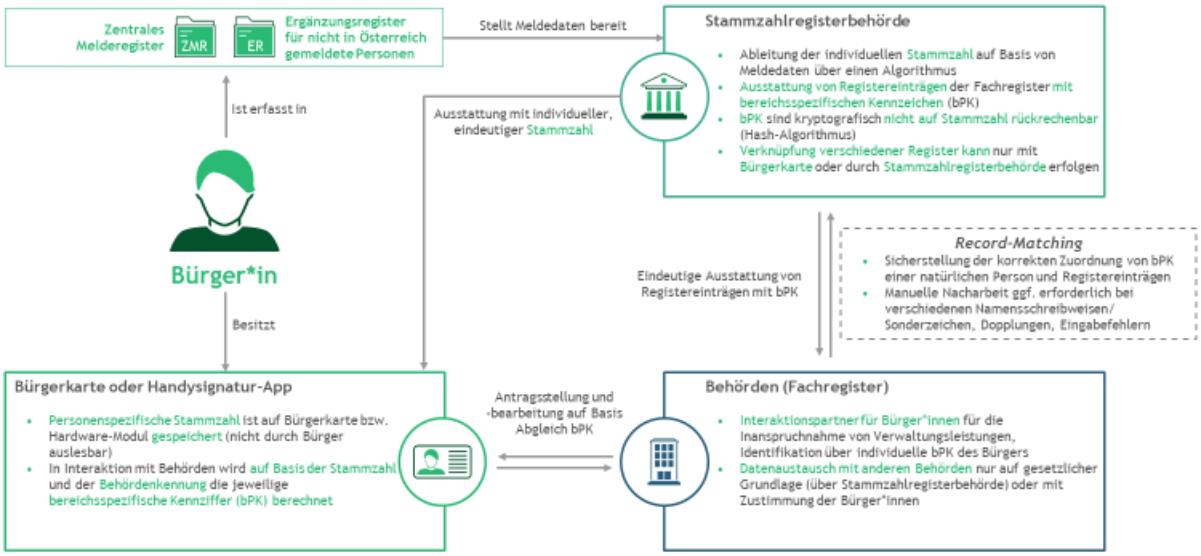


Abbildung 6: Verknüpfung von Stammzahl und bereichsspezifischen Kennzeichen in Österreich[30]

Die sektorübergreifende Nutzung von Identifikatoren ist im österreichischen Modell dadurch gewährleistet, dass Unternehmen eigene Bereichskennungen mit eigenen bPK anlegen können. Das österreichische E-Government-Gesetz sieht in diesem Fall die Stammzahl des Unternehmens als Bereichskennung vor. Da im Datenaustausch mit den Behörden durch die Stammzahlenregisterbehörde eine bPK erzeugt und verschlüsselt werden muss, wird dem Unternehmen ein entsprechender Kostenersatz in Rechnung gestellt. Der Nutzungsgrad von Datenaustauschverfahren mittels bPK durch die Wirtschaft wurde in Experteninterviews als gering eingeschätzt; gesicherte Zahlen dazu waren nicht verfügbar.

Da bei Einführung des Identifikatorensystems bereits elektronische Register bestanden, musste Österreich seine existierenden Register und Fachverfahren nachträglich mit Identifikatoren

[30] Die Abbildung zeigt den Prozess ausgehend von natürlichen Personen. Im Falle von nicht-natürlichen Personen funktioniert der Prozess analog. Anstatt allerdings auf das zentrale Melderegister zuzugreifen, greift die Stammzahlenregisterbehörde hier auf das Firmenbuch, das Vereinsregister oder das Ergänzungsregister zu.

ausstatten. Die Verknüpfung der Identifikatoren und Registerdaten erfolgte schrittweise und ist bis heute nicht vollständig abgeschlossen. Bei erstmaligem Kontakt mit einer Behörde kann es dazu kommen, dass dem Identifikator keine Daten aus dem Register zugewiesen werden können. Dann ist eine nachträgliche, manuelle Bearbeitung notwendig. Die Herausforderung des „Record-Matching“ besteht für jedes System, das bereits existierende Dateneinträge in verschiedenen Registern über einen einheitlichen Identifikator oder verschiedene bereichsspezifische Identifikatoren verknüpfbar machen möchte.

Während sich als positiver Nebeneffekt des Record-Matching automatisch die bereichsübergreifende Datenqualität verbessern lässt, ist der hierfür erforderliche initiale Aufwand erheblich: In Österreich waren laut Experteneinschätzung bei etwa 5 bis 10 % der erstmaligen Bildungen von bPK manuelle Nacharbeiten notwendig.[31] Dieser Aufwand ist daher nicht zu unterschätzen und muss in jedem Falle bei der Einführung von Identifikatoren berücksichtigt werden – das ist eine der wesentlichen Lehren der österreichischen Umsetzungserfahrung.

Bewertung des österreichischen Modells

Ähnlich dem estnischen System dient auch der österreichische Identifikator primär der Optimierung der Interoperabilität zwischen verschiedenen staatlichen Registern. Durch die Stammzahl und die ergänzenden bPK soll ein medienbruchfreier, eindeutiger Austausch von personenbezogenen Informationen auf höchstem datenschutzrechtlichen Niveau ermöglicht werden.

(1) Nutzbarkeit

Bedingt durch die historisch gewachsene Grundkomplexität der Ausgestaltung von Identifikatoren im österreichischen Modell ist die Nutzbarkeit in einigen wenigen Fällen eingeschränkt bzw. nicht gegeben. Als Beispiel mit erheblicher Tragweite sei die fehlende Möglichkeit zur einfachen Verknüpfung physischer und elektronischer Identitäten aufgrund nicht existierender öffentlicher Identifikatoren genannt. Verstärkt wird dieser Effekt zudem durch die Trennung der Bürgerkarte als elektronisches Identifizierungsmittel vom Personalausweis. Ein weiteres Beispiel für die eingeschränkte Nutzbarkeit ist die fehlende Möglichkeit der Verwendung des Identifikators als Nutzername. Da bei der österreichischen Handysignatur stattdessen die Handynummer als Benutzername fungiert, hat dies jedoch keine nennenswerten Auswirkungen.

[31] Angabe aus Experteninterview des Projektteams.

Eine sektorübergreifende Nutzung des Systems sowie die Vergabe von Rollen und Rechten sind im österreichischen Modell möglich.

(2) Einfachheit

Die komplexere Ausgestaltung des österreichischen Identifikatorensystems hat vor allem Auswirkungen auf die Einfachheit der Erstellung und Weiterentwicklung von digitalen Services. Aus der Perspektive von Diensteanbietern erschwert die Ausgestaltung der Identifikatoren nicht nur den ressourcenschonenden und einfachen Datenaustausch, sondern erhöht darüber hinaus die technische Komplexität der Anwendungen für digitale Dienste. Laut Expertenmeinung sei in Österreich zu erkennen, dass sich Komplexität potenziere: Werde ein komplexes Grundsystem etabliert, nehme die Komplexität mit jeder Erweiterung zu.[32] Dieser Umstand erschwert mit hoher Wahrscheinlichkeit auch die kontinuierliche Anpassung des Systems an technische Fortschritte.

Nach Aussagen von österreichischen Experten wurde zuletzt in Fachkreisen eine Vereinfachung des österreichischen Identifikatorensystems diskutiert. Experten bemängeln am gegenwärtigen System, dass insbesondere die hohe Anzahl der Verfahrensbereiche die Komplexität von Fachverfahren steigert. Fachverfahren, die elektronisch Daten mit anderen Bereichen austauschen, müssen für alle gespeicherten Personen die vbPK aus den entsprechenden Zielbereichen vorhalten. In diesem Zusammenhang wurde in Fachkreisen eine deutliche Reduktion der Verfahrensbereiche von 35 auf vier oder fünf erwogen, um die Komplexität des Systems zu verringern. Dies würde jedoch die Hürden der Zusammenführung persönlicher Daten im System reduzieren und Sinn und Zweck der zusätzlichen technischen und prozessualen Komplexität des Systems in Frage stellen.

Die Auswirkungen des Identifikatorensystems auf die Einfachheit aus Nutzerperspektive lassen sich ohne umfängliche Vergleiche der konkreten Umsetzung analoger Anwendungsfälle nur schwer beurteilen. Beispielhaft kann angeführt werden, dass die Zuweisung von Rollen und Rechten mit der Eingabe einer größeren Zahl an Basisdaten der Person verbunden ist, da eine zweifelsfreie Zuordnung nicht über den Identifikator vorgenommen werden kann.

Zudem ist davon auszugehen, dass die Ausgestaltung des österreichischen Modells die Einfachheit der Nutzung von Datenaustauschverfahren durch die Wirtschaft mindert. Auch dürfte es eher mehr Zeit beanspruchen, Effizienzpotenziale automatisierter Datenaustauschverfahren zwischen Wirtschaft und Staat zu realisieren.

---

[32] Angabe aus Experteninterview des Projektteams.

(3) Vertrauenswürdigkeit

Der Schutz personenbezogener Daten hat im österreichischen Identifikatorensystem oberste Priorität und bildet die Vertrauensgrundlage zwischen Staat und Bürger*innen. Das Modell erfüllt damit nicht nur regulatorische Vorgaben zur Vermeidung der Zusammenführung persönlicher Daten, sondern trägt auch kulturellen Erwartungen Rechnung.

In der Praxis wird der angestrebte Effekt im Hinblick auf den Datenschutz allerdings nur bedingt erreicht. Nach Expertenangaben schränkt die weiterhin bestehende Speicherung von persönlichen Daten, wie Namen und Geburtsdaten, in Registern und Fachanwendungen den positiven Effekt auf die Verhinderung der Profilbildung deutlich ein.[33] Der Erfolg des österreichischen Systems in Hinsicht auf die Vertrauenswürdigkeit liegt folglich nicht darin, dass der Datenschutz gegenüber dem Ausgangszustand vor Einführung der Identifikatoren verstärkt, sondern eher darin, dass er nicht verschlechtert wurde.

Zur Verbesserung des Datenschutzes und der Vertrauenswürdigkeit im Zusammenhang mit der Einführung von Identifikatoren könnten andere Maßnahmen besser geeignet sein. Insbesondere die Kontrolle über die Zugriffe auf persönliche Daten über ein Konsensmodul und die Nachvollziehbarkeit von Zugriffen über ein Datenschutzcockpit könnten die Vertrauenswürdigkeit gegenüber dem Status quo erhöhen.

Im gegenwärtigen österreichischen Modell darf die Verarbeitung einer Stammzahl zur Generierung eines bPK nur unter Mitwirkung des/der Betroffenen (z. B. durch Aktivierung des Verfahrens via Authentifizierung mittels Bürgerkarte oder Handysignatur) oder durch die Stammzahlenregisterbehörde im Auftrag des/der Betroffenen zur Datenermittlung, Amtshilfe etc. erfolgen. Im Kontext der Transparenz der Datenverarbeitung ergibt sich daher ein gewisses Maß an Nachvollziehbarkeit seitens der Bürger*innen. Im Vergleich zum estnischen Datenschutzcockpit erhalten die österreichischen Bürger*innen jedoch weitaus weniger Informationen über die Verarbeitung der Daten, insbesondere was den innerbehördlichen Datenaustausch anbelangt. Ein Konsensmodul zur effizienteren Verarbeitung von Daten, wie es im estnischen X-Road-System geplant ist, gibt es in Österreich derzeit nicht. Falls dort im Rahmen einer digitalen Behördendienstleistung eine explizite Zustimmung erforderlich ist, wird diese innerhalb der Anwendung abgefragt. Da die Verarbeitung einer Stammzahl zur Generierung eines bPK nur unter Mitwirkung oder im Auftrag des/der Betroffenen erfolgen kann, ist eine Datensouveränität in hohem Maße gegeben.

---

[33] Im Rahmen des Once-Only-Prinzips ist Österreich allerdings bestrebt, Register im Sinne der Datenminimierung landesweit umzugestalten, um so das angestrebte Maß an Datenschutz auch in der Praxis zu gewährleisten.

Zusammenfassend lässt sich feststellen, dass die österreichische Ausgestaltung ein hohes Maß an Datenschutz sowie an Rechtssicherheit garantiert. Mit dem Weg der verschlüsselten, für Einzelbehörden nicht rückrechenbaren bPK soll verhindert werden, dass Daten aus verschiedenen Registern zu Persönlichkeitsprofilen verknüpft werden. Gleichzeitig ist ein umfassendes System des innerbehördlichen Datenaustauschs geschaffen worden, das dem Bürger zudem erlaubt, eigene Registerdaten auch mit privaten Anbietern zu teilen. Es zeigt sich jedoch, dass die relativ komplexe organisatorische und technische Ausgestaltung des österreichischen Systems und insbesondere das Fehlen eines öffentlichen Identifikators die Komplexität bei der Umsetzung weiterer Anwendungsfälle erhöhen. Die gleichen Umstände führen überdies dazu, dass eine vom Bürger gewünschte Nutzbarmachung von Registerinformationen für private Dienste erschwert wird. Dadurch büßen das eID-Ökosystem wie das Interoperabilitätssystem insgesamt an Attraktivität für die Anbietung privater Dienstleistungen ein.

3. Interoperabilitätssysteme im Ländervergleich

Nachdem mögliche Ausgestaltungsansätze von Identifikatoren anhand der Länderbeispiele Estland und Österreich beleuchtet wurden, soll abschließend auf die unterschiedlichen Grade des Datenaustauschs sowohl zwischen staatlichen als auch nichtstaatlichen Organisationen in den jeweiligen Interoperabilitätssystemen eingegangen werden. Um die direkte Verknüpfung zwischen der Ausgestaltung von Identifikatoren und den verschiedenen Stufen des Datenaustauschs zu ermöglichen, bedient sich das Stufenmodell u.a. der Länder Estland und Österreich als beispielhafte Vertreter einer Stufe. Abbildung 7 stellt die unterschiedlichen Grade des Datenaustauschs zwischen staatlichen Behörden in fünf Stufen dar. Beginnend mit Stufe 0 nehmen mit jedem Grad Umfang und Effizienz des Austauschs von Daten zu. Allerdings geht dabei wachsende Effizienz nicht zwingend mit zunehmender Vertrauenswürdigkeit aus Sicht der Bürger*innen einher. So erfolgt beispielsweise auf Stufe 4 der freie Datenaustausch auf Kosten der Datensouveränität.

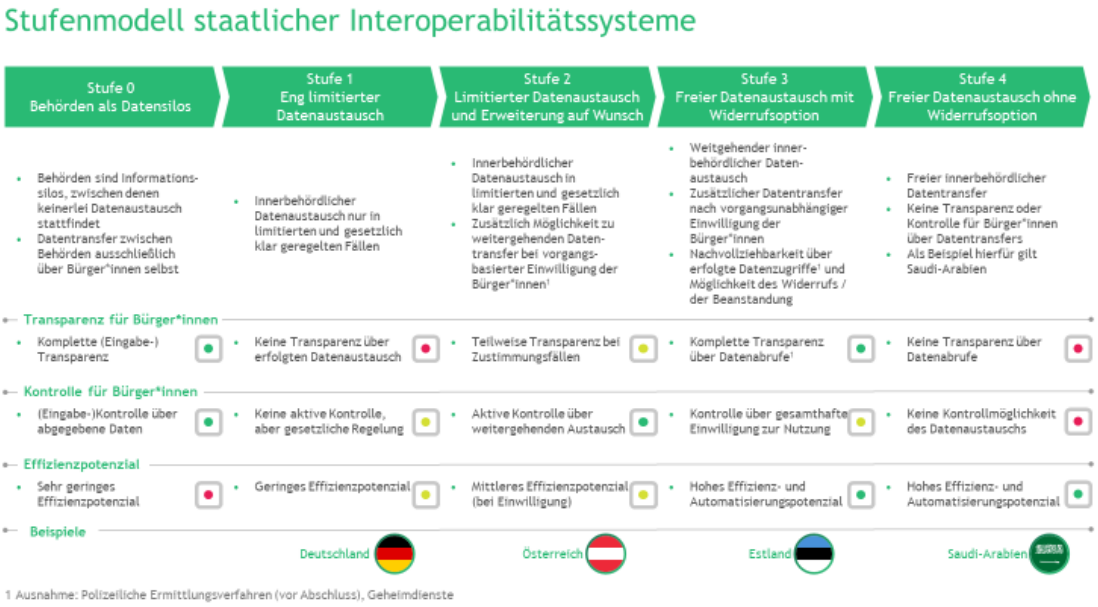


Abbildung 7: Stufenmodell staatlicher Interoperabilitätssysteme

Während auf **Stufe 0** die Daten in Silos gespeichert werden und der Datentransfer ausschließlich über die Bürger*innen selbst erfolgt, werden auf **Stufe 1** Daten in limitierten, gesetzlich klar geregelten Fällen zwischen Behörden ausgetauscht. Auf dieser Stufe lässt sich das aktuelle System Deutschlands einordnen. Vor allem im Kontext der zunehmenden Digitalisierung der Behörden und der aktuellen Umsetzung des OZG wäre es für Deutschland erstrebenswert, das System in Richtung der Stufen 2 und 3 weiterzuentwickeln. Das österreichische Modell ist auf der **Stufe 2** zu verordnen. Diese beinhaltet neben den gesetzlich geregelten Fällen die Möglichkeit der Einwilligung der Bürger*innen zu einem registerübergreifenden Datentransfer. Auf **Stufe 3** des Datenaustauschmodells gibt es eine große Zahl gesetzlich geregelter Fälle von elektronischem Datenaustausch zwischen Behörden und mit nichtstaatlichen Organisationen. Zusätzlich ist die Genehmigung zum Austausch von Daten insbesondere bei privaten Anbietern in vielen Fällen an die Akzeptanz von Nutzungsbedingungen geknüpft. Gleichzeitig wird weitgehende Transparenz über die erfolgten Datenzugriffe gewährt. Beispielhaft für diese Form des Datenaustauschs ist der Kauf von Monatskarten für den kostenlosen öffentlichen Nahverkehr in Estlands Hauptstadt Tallinn. Die kostenlose Nutzung gilt dabei nur für in Tallinn gemeldete Personen. Die Inhaber von Monatskarten müssen daher einwilligen, dass regelmäßig elektronisch überprüft werden darf, ob sich ihr Hauptwohnsitz in Tallinn befindet. In ihrem Datenschutzcockpit können die Bürger*innen jedoch die monatliche Überprüfung ihres Wohnsitzes durch den ÖPNV-Betreiber nachvollziehen. Auf der letzten **Stufe 4** findet ein freier Datenaustausch ohne individuelle Kontrolle oder Nachvollziehbarkeit statt. Alle Behörden können die bei ihnen gespeicherten persönlichen Daten ohne Beschränkung untereinander austauschen. Auf dieser Stufe spielen Transparenz und Datenschutz im Rahmen des Datenaustauschs also keine Rolle.

6. Handlungsempfehlungen

Wie bereits vor der Einführung der steuerlichen Identifikationsnummer im Jahr 2007 findet die aktuelle Debatte um die Etablierung eines Identifikators in Deutschland bisher weitestgehend unbeachtet von der Öffentlichkeit statt. Dabei steht für Bürger*innen sowohl auf der Chancen-als auch der Risikoseite viel auf dem Spiel. Die Ausgestaltung persönlicher Identifikatoren im Rahmen des Registermodernisierungsgesetzes wird die Digitalisierung der deutschen Gesellschaft über die nächsten Jahrzehnte nachhaltig beeinflussen.

Verknüpfbare Identifikatoren erlauben es dem Staat, seine bestehende Datengrundlage auf ein zeitgemäßes Qualitätsniveau zu heben, sie vereinfachen die elektronische Authentifizierung und vor allem den automatisierten Austausch persönlicher Daten über Registergrenzen hinweg. Automatisierte Datenaustauschverfahren sind notwendig, um die Bearbeitungszeiten von Verwaltungsleistungen zu reduzieren und neuartige Ansätze, wie beispielsweise antragslose Verfahren, zu ermöglichen. Für die Zukunftsfähigkeit der öffentlichen Verwaltung in Deutschland sind sie unerlässlich.

Zugleich können Identifikatoren und ein automatisierter Datenaustausch aber das Vertrauen der Bürger*innen in den Staat schädigen und Befürchtungen vor unrechtmäßigen Zusammenführungen von sensiblen persönlichen Daten wecken. Neben potenzieller Ablehnung aus der Bevölkerung besteht die größte Hürde für die Einführung von Identifikatoren in der Unklarheit über die rechtliche Zulässigkeit verschiedener Gestaltungsoptionen. Grundsätzlich lässt sich sagen, dass in Abhängigkeit von den mit einer Gestaltungsoption verbundenen Risiken angemessene Schutzmaßnahmen zu treffen sind, die insbesondere den rechtlichen Geboten der Zweckmäßigkeit, Transparenz und des effektiven Rechtsschutzes genügen.[34] Demgemäß müssen, damit die Einführung von Identifikatoren in Deutschland nicht erneut scheitert, insbesondere das Vertrauen der Bevölkerung gewonnen und rechtliche Risiken durch angemessene Schutzmaßnahmen minimiert werden. Aufgrund der engen Verknüpfung von Identifikatoren und Interoperabilität müssen die Maßnahmen auch diese Bereiche adressieren.

Auf Basis der dargelegten Analysen, der vorstehend beschriebenen Erfahrungen mit der Umsetzung von Identifikatoren in anderen europäischen Staaten sowie der rechtlichen Risiken haben wir die im Folgenden angeführten Handlungsempfehlungen für Deutschland entwickelt.

---

[34] Vgl. Martini/Wagner/Wenzel (2017): Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern.

1. Leitlinien

1. **Vertrauenswürdigkeit durch Transparenz und aktive Kontrolle schaffen**
   Um das Vertrauen der Bürger*innen zu gewinnen und Rechtssicherheit für die Einführung von Identifikatoren und den zunehmenden Austausch von persönlichen Daten herzustellen, sollten weitestgehende Kontrolle und Transparenz über die Speicherung und den behördenübergreifenden Austausch von Daten geschaffen werden (vgl. 4.9 und 4.10). Zudem sollten Bürger*innen das Recht haben, nachgelagert Auskunft über sämtliche Zugriffe auf ihre persönlichen Daten einzuholen, um deren Rechtmäßigkeit nachvollziehen zu können (vgl. 4.6). Zugriffe auf, Speicherung und behördenübergreifender Austausch von Daten müssen auch zukünftig auf das notwendige Minimum begrenzt bleiben, um eine unrechtmäßige Zusammenführung persönlicher Daten zu verhindern. Dazu sind adäquate Schutzmaßnahmen zu etablieren.

2. **Komplexität langfristig minimieren**
   Die Ausgestaltung von Identifikatoren hat maßgeblichen Einfluss auf die Komplexität aller Systeme, die sie zukünftig nutzen. Dies betrifft große Teile der deutschen Registerlandschaft, elektronische Identifizierungsmittel, Interoperabilitätssysteme, sämtliche Fachanwendungen, die Daten behördenübergreifend austauschen, sowie Systeme nichtstaatlicher Organisationen, die rechtmäßig auf Behördendaten zugreifen wollen. Um die Mehrwerte einer Vielzahl von Digitalisierungsinitiativen zeitnah und effizient realisieren zu können, sollte die Komplexität der Identifikatoren und damit verbundener Schutzmechanismen im Interoperabilitätssystem im Rahmen des rechtlich Möglichen minimiert werden (vgl. 2.1). Damit die Erfolgschancen der Einführung von Identifikatoren nicht gemindert werden, sollten Identifikatoren und verwandte Systeme auf bewährten Technologien, wie etwa Public-Key-Infrastrukturen, beruhen. Der Einsatz unerprobter Technologien, wie z. B. Self-Sovereign Identities, würde die Komplexität signifikant erhöhen.

3. **Sektorübergreifende Nutzbarkeit ermöglichen**
   Die Einführung von Identifikatoren darf nicht isoliert als reines Thema der Innenverwaltung betrachtet werden. Die Stärkung des deutschen eID-Ökosystems und der Interoperabilität von Registern bietet ebenfalls enormes Potenzial für den Privatsektor. Daher sollte die Ausgestaltung der Identifikatoren in Deutschland eine einfache, rechtskonforme Nutzung durch den Privatsektor vorsehen (vgl. 2.1). Dennoch bedarf die Nutzung von Identifikatoren und Interoperabilitätssystemen durch den Privatsektor besonderer Schutzmechanismen, um unrechtmäßige

Datenzugriffe zu verhindern. Sie sollte daher ausschließlich im Auftrag und mit expliziter Zustimmung der Bürger*innen möglich sein (4.9).

2. Ausgestaltung des Identifikators

1. Einheitliche oder bereichsspezifische Identifikatoren

Die wohl grundlegende Entscheidung bei der Einführung von Identifikatoren liegt in der Wahl zwischen einem Modell mit einem einheitlichen Identifikator, und einem Modell mit bereichsspezifischen Identifikatoren. Ersteres zielt auf eine Maximierung von Nutzbarkeit und Einfachheit ab, während ein bereichsspezifisches System vor allem maximale Vertrauenswürdigkeit anstrebt. In der bisherigen Diskussion in Deutschland hat sich das bereichsspezifische System aufgrund der Begünstigung des Datenschutzes durch seine technische Gestaltung als Favorit herauskristallisiert.[35] Im Kabinettsbeschluss des Registermodernisierungsgesetzes wurde jedoch ein einheitlicher Identifikator gewählt.

Als Ergebnis der näheren Betrachtung des bereichsspezifischen Modells Österreichs ist zu hinterfragen, ob die Steigerung der Vertrauenswürdigkeit und Rechtmäßigkeit in einem ausgewogenen Verhältnis zur erhöhten Komplexität steht. Anzumerken ist, dass der „Privacy by Design"-Effekt des österreichischen Systems in der Praxis erst voll zum Tragen kommen kann, wenn neben den bPK keine persönlichen Stammdaten mehr in verschiedenen Registern und Fachanwendungen gespeichert würden, die unregulierte behördenübergreifende Zusammenführungen von Daten erlauben. Es ist fraglich, ob ein solcher Zustand selbst im Zuge von Once-Only, insbesondere bei Fachanwendungen, überhaupt erreichbar ist. Zudem muss beachtet werden, dass eine Reduktion der Anzahl der Verfahrensbereiche – welche mit Blick auf die Komplexität des österreichischen Systems für Deutschland als Option diskutiert wird – die Vertrauenswürdigkeit des Systems insgesamt im Vergleich zum einheitlichen Identifikator wohl nur geringfügig erhöhen würde, da eine unrechtmäßige Zusammenführung einer Vielzahl persönlicher Daten durch die bPK sich nicht mehr effektiv verhindern ließe.

Die Einführung von einheitlichen Identifikatoren erleichtert zwar inhärent die Verknüpfung von persönlichen Daten, jedoch ist eine weitgehende Zusammenführung dieser Daten aus unterschiedlichen Registern mit den heutigen technischen Möglichkeiten moderner Big-Data-Anwendungen auch anhand persönlicher

[35] Vgl. Martini/Wagner/Wenzel (2017): Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, S. 34; Schaar: Revival des allgemeinen Personenkennzeichens? https://www.eaid-berlin.de/revival-des-allgemeinen-personenkennzeichens/

Stammdaten möglich. Der zusätzliche Effekt der Identifikatoren liegt vor allem in der Ermöglichung eines effizienten, synchronen Datenaustauschs aufgrund der Minimierung manueller Nacharbeiten für das Record-Matching.

Die Entscheidung für eines der Modelle wird trotz dieser Argumente vermutlich vor allem unter Berücksichtigung rechtlicher Gesichtspunkte erfolgen müssen, um das Risiko eines Scheiterns zu minimieren. Im Vergleich zum Status quo würde sowohl die Einführung einheitlicher als auch bereichsspezifischer Identifikatoren eine Verbesserung bedeuten. Prinzipiell ist die Nutzung einheitlicher, nicht-geheimer Identifikatoren unter Verwendung adäquater Schutzmechanismen aufgrund der höheren Nutzbarkeit, geringeren Komplexität und faktisch geringen Unterschiede im Bereich der Vertrauenswürdigkeit zu bevorzugen. Dies sollte jedoch nur angestrebt werden, sofern eine rechtlich weitgehend unbedenkliche Kombination aus einheitlichen Identifikatoren und Schutzmaßnahmen gefunden werden kann. Ist dies nicht der Fall, stellen bereichsspezifische Identifikatoren eine gute Alternative dar, sofern die Anzahl der Verfahrensbereiche und die damit verbundene Komplexität auf das notwendige Minimum reduziert werden können. In diesem Fall könnte eine treuhänderische zentrale Instanz die reine Zuordnung der jeweiligen bereichsspezifischen Kennziffern zueinander kennen und herstellen, ohne dabei am inhaltlichen Datenaustausch beteiligt zu sein. Ebenfalls denkbar wäre der Einsatz eines Konsensmoduls an zentraler Stelle, über welches die Bürger*innen ihre explizite Zustimmung zum Datenaustausch erteilen (vgl. 4.9).

3. Einführung des Identifikators

1. **Identifikator auf bestehenden Infrastrukturen aufsetzen**

   Bei der Entscheidung für einen einheitlichen Identifikator sollte die Steuer-ID als Grundlage für eine Ableitung des neuen Identifikators genutzt werden. Ähnlich zum österreichischen zentralen Melderegister ist sie aufgrund der hohen Datenqualität und Zugänglichkeit an einer zentralen Stelle die geeignetste Quelle für eine Ableitung mit geringer Komplexität. Bei der Entscheidung für bereichsspezifische Identifikatoren sollten, soweit möglich, die in einigen Registern schon existierenden bereichsspezifischen Identifikatoren (z. B. die Rentenversicherungsnummer) genutzt werden.

2. **Ausreichend Ressourcen für die Einführung der Identifikatoren bereitstellen**

   Unabhängig von der konkreten Ausgestaltung der Identifikatoren wird ihre Einführung einen enormen Aufwand mit sich bringen. Dies betrifft nicht nur die Einrichtung und den Betrieb eines zentralen Identitätsregisters, sondern vor allem das

Nachpflegen der Identifikatoren in den verschiedenen Fachregistern. Auf Grundlage der österreichischen Erfahrungen ist davon auszugehen, dass dies nicht in allen Fällen vollautomatisch möglich sein wird und ein Anteil von etwa 5 bis 10 % der Erstanfragen manuelle Eingriffe für das „Record-Matching" erfordert.[36] Der Zwischenbericht zum registerübergreifenden Identitätsmanagement für die Innenministerkonferenz adressiert dieses Thema nicht explizit, sondern lässt nur erahnen, dass es ein Team zur Datenpflege im zentralen Identitätsregister geben soll. Jedoch müssen auch Ressourcen für die Fachregister bereitgestellt werden, um das manuelle Record-Matching in einem angemessenen Zeitrahmen zu ermöglichen. Andernfalls besteht das Risiko, dass ein gewisser Anteil der Datenanfragen erst nach längeren Zeiträumen beantwortet werden kann.

3. Phasenweise Umsetzung des „Record-Matching" planen

Die Einführung von Identifikatoren sollte in mehreren Phasen geplant werden. In der Startphase sollten diejenigen Register, bei denen eine besonders hohe Relevanz für behördenübergreifende Datenaustauschverfahren vermutet wird – wie z. B. die örtlichen Melderegister, zentrale Fahrzeugregister und Handelsregister[37] – vollständig mit Identifikatoren ausgestattet werden. Register mit einer geringen Relevanz für behördenübergreifende Datenaustauschverfahren sollten entweder nur anlassbezogen oder nachgelagert mit Identifikatoren ausgestattet werden. Hierbei ist darauf hinzuweisen, dass selbst bei erheblichem Ressourcenaufwand die Umsetzung des „Record-Matching" für ein Land von der Größe und administrativen Unterteilung Deutschlands vermutlich mehrere Jahre in Anspruch nehmen dürfte. Aus diesem Grund kommt der richtigen Priorisierung der Register in der Umsetzungsplanung eine Schlüsselrolle zu.

4. Schutzmechanismen im Interoperabilitätssystem

Organisatorische und rechtliche Maßnahmen

1. Auf- bzw. Ausbau eines einheitlichen Interoperabilitätssystems und verpflichtende Nutzung für Behörden

---

[36] Ähnliche Erfahrungen sind auch in Deutschland bereits im Kontext der Einführung der einheitlichen Steuer-Identifikationsnummer 2008 gemacht worden, in deren Zuge zur Vergabe eindeutiger Identifikationsnummern z. B. Datenduplikate entfernt werden mussten.

[37] Vgl. Normenkontrollrat (2017): Mehr Leistungen für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, S. 10 ff.

Um eine effektive Kontrolle über den elektronischen Datenaustausch zwischen Behörden zu etablieren, sollte ein einheitliches Interoperabilitätssystem für den innerbehördlichen und sektorübergreifenden Datenaustausch in Deutschland aufgebaut werden. Für Behörden muss die Nutzung dieses Systems für den elektronischen Datenaustausch nach einer Übergangsfrist verpflichtend sein. Der Aufbau eigener Schnittstellen außerhalb dieses Interoperabilitätssystems darf dann nicht mehr zulässig sein. Das Interoperabilitätssystem könnte auf bestehenden Strukturen, insbesondere dem Deutschen Verwaltungsdiensteverzeichnis (DVDV), aufsetzen.

2. **Zentrale Stelle zur Steuerung des Zugangs zum Interoperabilitätssystem schaffen**

Für die Steuerung des Interoperabilitätssystems sollte eine zentrale Stelle geschaffen werden, die für Entwicklung, Betrieb und Governance des Systems zuständig ist. Mit Blick auf die Schutzmechanismen sollte diese Stelle den Zugang von Organisationen zum Interoperabilitätssystem auf der Basis rechtlich festgeschriebener Kriterien, beispielsweise durch die Ausgabe von Zertifikaten, kontrollieren.[38] Gleichwohl sollte der Registrierungsprozess für Organisationen im Rahmen der gebotenen Vorsicht möglichst einfach gehalten werden, um einen schnellen Hochlauf der angebundenen Organisationen und somit auch der Nutzbarkeit des Systems zu begünstigen.

3. **Prüfung der Zulässigkeit von Datenteilungsverfahren und Datenkonsumenten durch Datenanbieter**

Die Entscheidung über das Teilen von Daten sollte beim Datenanbieter bzw. der registerführenden Stelle liegen. Diese sollte unter Einbindung der Datenschutzbeauftragten die Einrichtung aller neuen Datenteilungsverfahren für das jeweilige Register sowie die Zulassung aller Datenkonsumenten verantworten. Die Zustimmung des Datenschutzbeauftragten sollte Voraussetzung für die Inbetriebnahme des Verfahrens und dessen Bekanntmachung in einem zentralen Diensteverzeichnis wie dem DVDV sein.

4. **Unabhängige Stelle für Auditierung von Datenservices**

Die allgemeine Zulässigkeit der Datenaustauschverfahren innerhalb des Interoperabilitätssystems sollte durch eine unabhängige Stelle, beispielsweise beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, regelmäßig

[38] Um dem System beitreten zu können, sollten Organisationen rechtlich festgeschriebene Kriterien erfüllen müssen (z. B. rechtliche Grundlage für Datenaustauschverfahren, konkreter Anwendungsfall, der – beispielsweise durch die Verwendung eines Konsensmoduls – allgemeinen rechtlichen Anforderungen genügt; nachweisliche Erfüllung von IT-Sicherheitsstandards).

geprüft werden. Diese Stelle sollte auch das Recht haben, technische Audits der Effektivität technischer Schutzmechanismen im Interoperabilitätssystem durchzuführen oder zu beauftragen.

5. **Verankerung des Gebots der Datenminimierung im Interoperabilitätssystem**

   Die Operationalisierung des Prinzips der Datenminimierung sollte in Bezug auf Datenaustauschverfahren innerhalb des Interoperabilitätssystems rechtlich bindend festgeschrieben werden. Dabei sollte darauf abgezielt werden, dass Datenanbieter ihre Datenteilungsverfahren so einrichten, dass jeweils nur die zwingend notwendigen Informationen für die Entscheidungsfindung beim Datenkonsumenten weitergegeben werden dürfen.[39]

6. **Verankerung eines Rechts auf Auskunft über Datenzugriffe**

   Ein Recht auf Auskunft über behörden- und sektorübergreifende Zugriffe auf persönliche Daten über das Interoperabilitätssystem sollte rechtlich verankert werden und durch geeignete technische Maßnahmen nutzerfreundlich realisiert werden (vgl. 4.10). Dabei sollte auch vorgeschrieben werden, dass langfristig nachvollziehbar sein muss, welche konkrete Person eine behördenübergreifende Datenanfrage ausgelöst hat, sofern diese manuell ausgelöst wurde. Zudem sollte der Grund für die Anfrage nachvollziehbar dokumentiert werden.[40]

7. **Speicherung des Identifikators in der Privatwirtschaft nur mit ausdrücklicher Zustimmung**

   Es sollte gesetzlich festgeschrieben werden, dass Unternehmen Bürger*innen im Rahmen der Inanspruchnahme von Leistungen nicht zur Angabe ihres Identifikators verpflichten können. Die Speicherung des Identifikators muss auf Freiwilligkeit und ausdrücklicher Zustimmung der Bürger*innen beruhen. Zudem sollten Bürger*innen die Löschung ihres Identifikators bei Unternehmen unkompliziert veranlassen können.

8. **Gerichtsfeste Dokumentation des Datenverkehrs durch Datenanbieter und -konsumenten**

   Datenanbieter und Datenkonsumenten sollten über das Interoperabilitätssystem gesendete bzw. erhaltene Datenabfragen und Antworten vollständig[41] als gerichtsfeste Dokumente langfristig und sicher in ihren eigenen Systemen speichern. Dies ist

---

[39] Will beispielsweise ein Nahverkehrsunternehmen beim Online-Verkauf eines Studententickets nachprüfen, ob der Käufer tatsächlich aktuell an einer Hochschule immatrikuliert ist, sollte ein einfaches „Ja“ des Datenanbieters genügen. Die Preisgabe der Hochschule darf in diesem Fall nicht zulässig sein.

[40] Für die Darstellung der Gründe wären denkbar: die rechtliche Grundlage für den Datenaustausch, die relevante Verwaltungsleistung und die Vorgangsnummer.

[41] D. h. inklusive des Inhalts der Anfragen und Antworten sowie insbesondere auch der Zustimmung zum Datenaustausch durch Bürger*innen.

notwendig, um (1) die Zustimmung von Bürger*innen zum Datenaustausch beweisen zu können und (2) den Inhalt von Datenanfragen und Antworten im Falle rechtlicher Streitigkeiten über Entscheidungen, die unter Einbeziehung von über das Interoperabilitätssystem bereitgestellten Daten getroffen wurden, als Beweise verwenden zu können. Letzteres ist vor allem notwendig, um die Akzeptanz für die Nutzung solcher Verfahren bei den Datenkonsumenten zu steigern.

Technische und prozessuale Maßnahmen

9. Weitgehende Kontrolle über den Zugriff auf persönliche Daten gewähren

Bürger*innen sollten den Zugriff auf ihre persönlichen Daten weitestgehend selbst kontrollieren können. Für Datenzugriffe, die durch eine Online-Antragstellung von Bürger*innen ausgelöst werden, sollte die Zustimmung im Rahmen des Antrags im Sinne einer Vollmacht zum behördenübergreifenden Datenzugriff erteilt werden müssen.[42]

In bestimmten Konstellationen des behördenübergreifenden Zugriffs auf persönliche Daten sollte ein Konsensmodul an zentraler Stelle eingesetzt werden, um die Zustimmung zum Datenaustausch zu erteilen.[43] Der Zugriff von nichtstaatlichen Organisationen sollte immer eine explizite Zustimmung der Bürger*innen im Konsensmodul erfordern.

Der Zugriff auf persönliche Daten ohne explizite Zustimmung von Bürger*innen muss auf Basis einer rechtlichen Regelung weiterhin möglich sein. Diese Möglichkeit sollte jedoch möglichst sparsam, z. B. im Rahmen antragsloser Verfahren, genutzt werden.

10. Nachgelagerte Transparenz über Zugriffe auf persönliche Daten

Die Metadaten aller Anfragen nach personenbezogenen Daten in staatlichen Registern sollten unveränderbar und zugriffsgeschützt in einem Datenschutzcockpit gespeichert und nur für die jeweils betroffene Person einsehbar und nachvollziehbar sein. Dabei sollte insbesondere der Anlass für den Datenaustausch in einfach verständlicher

---

[42] Dabei sollte für Bürger*innen in einfach verständlicher Weise aufgelistet werden, welche Daten von welchen Stellen angefragt werden.

[43] In spezifischen Fällen wird eine Zustimmung im Rahmen des Antragsverfahrens nicht ausreichend sein. Beispielsweise müssen beim BAföG-Antrag nicht nur persönliche Daten des Antragstellers, sondern auch sensible Finanzdaten der Eltern und Lebenspartner des Antragstellers übermittelt werden. Für solche Konstellationen wäre eine Zustimmung zum elektronischen Datenzugriff an zentraler Stelle für die weiteren Beteiligten ggf. einfacher als deren Einbindung in den Antragsprozess. Zudem könnte aufgrund der geringen Verbreitung von E-Signaturen die Nutzung eines zentralen Konsensmoduls eine E-Authentifizierung auf höherem Vertrauensniveau ermöglichen. Die Verwendung eines Konsensmoduls könnte zudem das politische Risiko der Einführung von Verfahren mit automatisiertem Datenaustausch für Entscheidungsträger reduzieren und damit die Verbreitung solcher Verfahren fördern.

Sprache enthalten und erkennbar sein, ob eine Antwort auf die Anfrage von dem Datenanbieter gesendet wurde.

11. Automatisierte Prüfung der Legitimität jeder Datenanfrage durch den Datenanbieter

Sofern die Datenabfrage durch eine Antragstellung von Bürger*innen ausgelöst wird, sollte die explizite Zustimmung (Vollmacht) zur elektronischen Abfrage der Daten der antragstellenden Person (idealerweise in Form einer elektronischen Signatur) der Datenabfrage beigefügt sein. Falls Identifikatoren zukünftig in Signaturzertifikaten enthalten sind, könnte die Bereitstellung der Daten von einem erfolgreichen Matching zwischen der Signatur in der Abfrage und dem Identifikator der abgefragten Daten abhängig gemacht werden.

Bei Anfragen auf Basis gesetzlicher Grundlage ohne explizite Zustimmung der antragstellenden Person sollten die Rechtsgrundlage und ein qualifiziertes Siegel der anfragenden Organisation mitgeschickt werden.

Bei Verwendung des Konsensmoduls zur Erteilung der Zustimmung durch Bürger*innen muss das Vorliegen der Zustimmung vom Datenanbieter unkompliziert überprüft werden können, bevor die Daten übermittelt werden.

12. Automatisierte Überwachung von Datenflüssen

Zusätzlich zur Durchführung von Audits der Datenservices (vgl. 4.4) sollte ein technisches System zur Überwachung der Datenflüsse im Interoperabilitätssystem etabliert werden. Hauptzweck dieses Systems sollte die Echtzeitüberwachung hinsichtlich datenschutzrechtlich auffälliger Muster sein, wie z. B. ein hohes Aufkommen von Anfragen zu einer bestimmten Person. Das System sollte diese Auffälligkeiten unmittelbar melden und so eine zeitnahe Überprüfung ermöglichen. Die Kontrolle und der alleinige Zugang zu diesem System sollten bei der unabhängigen Stelle zur Auditierung von Datenservices liegen (vgl. 4.4).