BMI - Referat V II 2
Berichtsdatum: 10. März 2020

Bundesministerium
des Innern, für Bau
und Heimat

Registerübergreifendes Identitätsmanagement
als Teil der Registermodernisierung

Abschlussbericht

zur Sondierung eines registerübergreifenden Identitätsmanagements mit Einbezug der Erfahrungen mit der Steuer-Identifikationsnummer für die Innenministerkonferenz 17. - 19. Juni 2020

Inhaltsverzeichnis

1. Der IMK-Auftrag zum registerübergreifenden Identitätsmanagement

Zum registerübergreifenden Identitätsmanagement hat die IMK drei Beschlüsse gefasst:

- Die Ständige Konferenz der Innenminister und -senatoren der Länder hat auf ihrer 209. Sitzung vom 28. bis 30.11.2018 in Magdeburg zu TOP 14 in Ziffer 2 folgenden Beschluss gefasst: „Davon ausgehend, dass verlässliche Angaben zur Identität von Personen die Grundlage für Verwaltungsleistungen darstellen, hält sie ein registerübergreifendes Identitätsmanagement und die Stärkung der Interoperabilität von Verwaltungsregistern in einer vernetzten Verwaltung für wesentliche Bestandteile einer Registermodernisierung.“ In Ziffer 3 bat die IMK das BMI darum, bis zur Frühjahrssitzung 2019 einen Vorschlag für die Verbesserung des Identitätsmanagements auszuarbeiten, der die Ausführungen zu TOP 5 "Digitalisierung der Verwaltung" der Jahreskonferenz der Regierungschefinnen und Regierungschefs der Länder vom 24. bis 26.10.2018 berücksichtigen sollte.
- In der 210. Sitzung vom 12. bis 14.06.2019 in Kiel zu TOP 12 bat die IMK in Ziffer 2 das BMI, auf Grundlage dieses Vorschlags die konzeptionellen Arbeiten unter Einbeziehung der Länder und der Koordinierungsstelle für IT-Standards (KoSIT) fortzuführen und in Ziffer 3 darum, ihr bis zur Herbstsitzung 2019 einen Zwischenbericht vorzulegen, der die erforderlichen Rechtsänderungen darstellt und Optionen für die fachliche und technische Realisierung eines registerübergreifenden Identitätsmanagements beinhalten soll.
- In der 211. Sitzung vom 4. bis 6.12.2019 in Lübeck zu TOP 32 bat die IMK das BMI um vorliegenden Abschlussbericht zu einer Sondierung einer möglichen Nutzung der Steuer-Identifikationsnummer, der ID-Nummer-Datenbank im Bundeszentralamt für Steuern und der dort eingerichteten Prozesse zur Qualitätsverbesserung als Basis für ein zukünftiges zentrales Identitätsregister unter Berücksichtigung des rechtlichen und technischen Anpassungsbedarfs.

Mit diesem Dokument wird die Sondierung nach Abstimmung in der Bund-Länder-Arbeitsgruppe Registerübergreifendes Identitätsmanagement und den Arbeitskreisen I und II mit ei-

nem Stand 10. März 2020 abgeschlossen. Im Ergebnis befürwortet die fachliche Bund-Länder-Arbeitsgruppe eine praxisnahe, auf bestehenden Strukturen aufsetzende, zügig realisierbare und gleichzeitig verfassungs- und datenschutzkonforme Lösung für ein registerübergreifendes Identitätsmanagement für die öffentliche Verwaltung mittels Verwendung der Steuer-Identifikationsnummer (Steuer-ID).

2. Anforderungen an ein registerübergreifendes Identitätsmanagement

2.1 Anforderungen aus Sicht der IMK

Der mit IMK-Beschluss vom 14.06.2019 gebilligte Vorschlag vom 11.02.2019 enthält fünf Anforderungen an ein registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung:

1. Eindeutige Zuordnung der Personalienidentität über alle Register hinweg durch Einführung eines Kerndatensystems mit Identifier: Die Grunddaten zu einer Person sollen an einer zentralen Stelle gespeichert, in Abstimmung mit den Fachregistern auf Inkonsistenzen geprüft, verlässlich gepflegt, aktualisiert und bereitgestellt werden. Hierfür wollen wir ein Kerndatensystem schaffen, in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden. Es wird zudem kenntlich gemacht, wie valide die Angaben zur Identität sind. Die Feststellung und Sicherung der Identität von Personen und die damit einhergehende Aufgabe zur Führung des Kerndatensystems soll eine eigenständige Aufgabe sein und einer eigenen Stelle zugeordnet werden. Eine eindeutige Zuordnung der Personalienidentität über alle Register hinweg ist herzustellen. Dies kann mithilfe eines Identifiers geschehen.
2. Auflösung von Datensilos: Jedes Datum sollte möglichst nur in einem Register der originär zuständigen Behörde vorhanden sein und von dieser gepflegt werden. Im Gegenzug muss sichergestellt werden, dass alle Behörden die Daten, die sie für ihre Aufgabenerfüllung benötigen, schnell und unkompliziert erhalten können und dürfen. Einmal erhobene Informationen stehen im Rahmen eines Rechte- und Rollenkonzepts für alle weiteren relevanten Zwecke im Rahmen der rechtlichen Vorgaben zur Verfügung.
3. Aktualität und Qualität sowie Datensicherheit und Datenschutz gewährleisten: Die Registerlandschaft sollte so weiterentwickelt werden, dass sie eine hohe Qualität und Aktualität der Registerdaten (z.B. durch Prüfung auf Doubletten und Inkonsistenzen, Über- und Untererfassungen) sowie die Zugänglichkeit des Datenbestands für die nutzenden Behörden aller föderalen Ebenen aufgabenadäquat sicherstellt. Zugleich sollte ein hohes Maß an Datensicherheit (z.B. durch physisch verteilte Datenhaltung)

und Datenverfügbarkeit gewährleistet sowie den datenschutzrechtlichen Vorgaben der EU-Datenschutz-Grundverordnung (nachfolgend DSGVO) sowie den hierzu ergangenen ergänzenden Regelungen und den verfassungsrechtlichen Vorgaben (insbesondere derjenigen des Rechts auf informationelle Selbstbestimmung) entsprochen werden.

4. Die für die Datenübermittlung bewährte Standardisierung (Standard X Inneres) soll fortentwickelt und auf die Registerstrukturen (Datenhaltung) ausgedehnt werden.
5. Transparenz: Die betroffenen Personen sollten im Rahmen ihres datenschutzrechtlichen Auskunftsrechts jederzeit auf einfache Weise feststellen können, welche Behörde zu welchem Zweck auf welche ihrer Daten zugegriffen hat.

Diese fünf Anforderungen gehen – insbesondere im vierten Punkt - über den Umfang der hier behandelten Sondierung eines zentralen Identitätsregisters („Kerndatensystem mit Identifier“) mit Einbeziehung der Steuer-ID hinaus und werden in nachfolgender fachlicher Aufbereitung und zusätzlichen Vorschlägen für Maßnahmen aufgegriffen.

2.2 Eckpunkte Digitalkabinett vom 18. November 2019

Nachdem sich entsprechend dem Ursprung des Vorhabens aus der IMK zunächst der Fokus der fachlichen Arbeit für ein registerübergreifendes Identitätsmanagement naturgemäß auf die Innenverwaltung richtete, wurde rasch deutlich, dass es sich um eine Basiskomponente für die Registermodernisierung und die OZG-Umsetzung insgesamt handelt. Damit erweiterte sich der Blickwinkel ab Herbst 2019 auf die anderen Ressorts. So hat das Bundeskabinett in seiner 76. Sitzung am 18. November 2019 „Eckpunkte zum registerübergreifenden Identitätsmanagement als Teil der Registermodernisierung“ beschlossen (s. Anhang 1). Wurde auch hier die Steuer-ID als Ausgangspunkt herangezogen, blieb die Frage der Verwendung eines einzigen oder mehrerer bereichsspezifischer Identifier zunächst offen. Neben einem „Basismodell“ wurden in der Folge zwei weitere konzeptionelle Modelle näher ausgearbeitet, um diese anhand einer Reihe von Kriterien, z.B. im Hinblick auf Verfassungs- und Datenschutzkonformität, Nutzen, Risiken und Realisierungsdauer besser bewerten zu können. In Kapitel 6 wird auf beide Modelle näher eingegangen, die Konzepte beider Modelle befinden sich aufgrund ihres Umfangs in einer separaten Anlage.

Neben den fachlichen Strängen der IMK und des Digitalkabinetts wurde das registerübergreifende Identitätsmanagement ebenfalls unter TOP 3.2 „Leitlinien für eine Modernisierung der Registerlandschaft“ der Besprechung der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder (MPK) am 5. Dezember 2019 behandelt und der Beschluss gefasst, dass sich die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der

Länder dafür einsetzen, dass die erforderlichen gesetzgeberischen Maßnahmen für ein registerübergreifendes Identitätsmanagement zeitnah auch unter dem Aspekt der Datensicherheit und des Datenschutzes geprüft und vorgestellt werden (Anhang 2).

2.3 Anforderungen aus anderen Ressorts

Nach der Erstellung und weiteren Ausarbeitung der beiden unterschiedlichen Modelle sowie einer zeitnah einberaumten Bewertungsrunde durch die Expertengruppen „Registerarchitektur“ und „Identifier“ wurde am 4. Februar 2020 zu einer ersten Ressortbesprechung eingeladen. Fachliche Anforderungen an die konzeptionellen Vorstellungen für das registerübergreifende Identitätsmanagement wurden aus den beteiligten Bundesministerien zunächst nicht übermittelt. Sie werden gegebenenfalls im Rahmen der Ressortabstimmung für das zu erstellende Artikelgesetz erwartet.

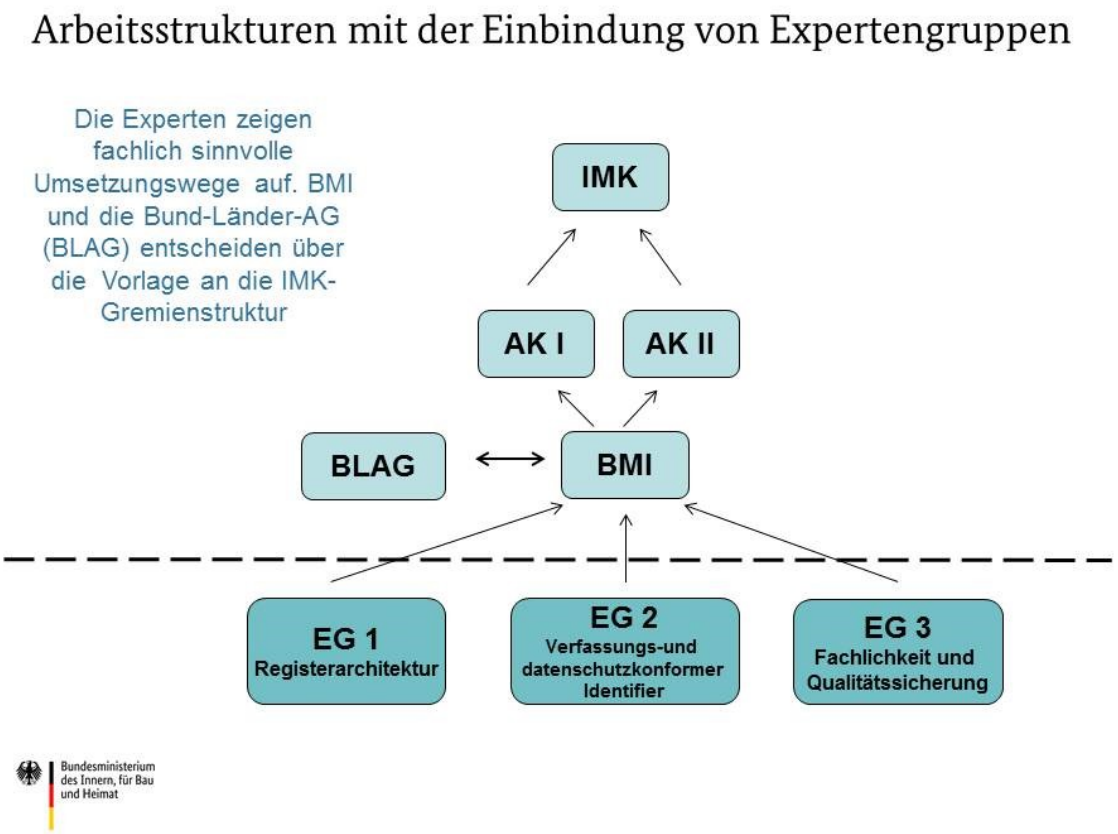
3. Die Arbeitsstruktur im Überblick

Nach dem ersten IMK-Beschluss vom 30. November 2018 wurde eine Bund-Länder-Arbeitsgruppe Registerübergreifendes Identitätsmanagement (im Folgenden: BLAG) unter der Federführung des BMI eingerichtet, in der die betroffenen Bereiche der Innenverwaltung, u.a. Meldewesen, Personenstandswesen, Ausländerwesen, Staatsangehörigkeitswesen, Pass- und Personalausweiswesen und die Statistik mit dem Ziel eingebunden wurden, den von der IMK erbetenen Vorschlag zur Verbesserung des Identitätsmanagements zu erarbeiten. Ebenso sind in der BLAG Vertreter des Vorsitzes des AK I, des AK II und des IT-Planungsrates repräsentiert.

Nach dem IMK-Beschluss vom 14. Juni 2019, auf der Grundlage des Vorschlags vom 11. Februar 2019 die konzeptionellen Arbeiten fortzuführen, wurden von der BLAG zur vertieften Bearbeitung der konzeptionellen Fragen drei beratende Expertengruppen errichtet:

- EG 1: Registerarchitektur
- EG 2: Verfassungs- und datenschutzkonformer Identifier
- EG 3: Fachlichkeit und Qualitätssicherung

In den Expertengruppen sind BMI und die Innenministerien der Länder mit den betroffenen Fachbereichen der Innenverwaltung sowie der für Digitalisierung verantwortlichen Stellen vertreten, zudem von diesen benannte Experten aus Behörden des Bundes und der Länder, der KoSIT und der Wissenschaft. Ebenso wurden im Hinblick auf die Erfahrungen mit der Steuer-ID im Bundeszentralamt für Steuern (BZSt) das BMF sowie - in der EG 2 im Hinblick auf Datenschutzfragen - das BMJV sowie die Kontaktgruppe „Registermodernisierung“ der Datenschutzkonferenz mit Vertretern des Bundesbeauftragen für Datenschutz und Informationsfreiheit (BfDI) sowie der Datenschutzbeauftragten der Länder beteiligt.



Grafik 1: Arbeitsstruktur im registerübergreifenden Identitätsmanagement

Um die beiden in Kapitel 6 behandelten Modelle für ein registerübergreifendes Identitätsmanagement aus einer ganzheitlichen Perspektive erstellen, weiter auszuarbeiten und bewerten zu können, wurden die Sitzungen der Expertengruppen 1 „Registerarchitektur“ und 2 „Identifier“ von Oktober 2019 bis Januar 2020 gemeinsam ausgerichtet.

4. Ein Identitätsregister mit numerischem Identifier

Als Ausgangspunkt der konzeptionellen Überlegungen für ein Basismodell wurde mit der ersten Anforderung des Vorschlags vom 11. Februar 2019 begonnen. Dies sind die Errichtung eines Kerndatensystems - im Folgenden als Identitätsregister bezeichnet - in dem die Basisdaten aller Personen mit Verwaltungskontakt gepflegt werden, und die Einführung eines verlässlichen und robusten Identifiers, der entsprechend Art. 87 DSGVO die Rechte und Freiheiten der Person wahrt und den verfassungsrechtlichen Anforderungen entspricht.

4.1. Ausgangslage in der Verwaltungspraxis

Verlässliche Angaben zur Identität von Personen sind die Basis aller Verwaltungsleistungen. Wird die Verwaltung zunehmend digitalisiert, muss auch in der digitalen Kommunikation gewährleistet sein, dass Personenverwechslungen ausgeschlossen sind und die betroffene

Person eindeutig identifiziert wird. Dies ist derzeit nicht der Fall. Vielfach kommt es in der digitalen Kommunikation zu Trefferlisten, in denen die Daten unbeteiligter Personen enthalten sind, oder zu einem Abbruch des digitalen Prozesses, weil die betroffene Person in einer Datenbank nicht eindeutig referenziert werden kann. Zudem werden derzeit häufig personenbezogene Daten, wie etwa die aktuelle Anschrift oder das Geburtsdatum einer Person, ausschließlich zu Zwecken der Identifikation übermittelt, obwohl sie für die eigentliche Aufgabenwahrnehmung entbehrlich sind. Deshalb ist es auch aus datenschutzrechtlichen Erwägungen heraus anzustreben, ein registerübergreifendes Identitätsmanagement einzuführen, das möglichst allen Behörden der öffentlichen Verwaltung aktuelle und korrekte personenbezogene Basisdaten für ihre Register bereitstellt und eine eineindeutige Zuordnung zu der betroffenen Person gewährleistet.

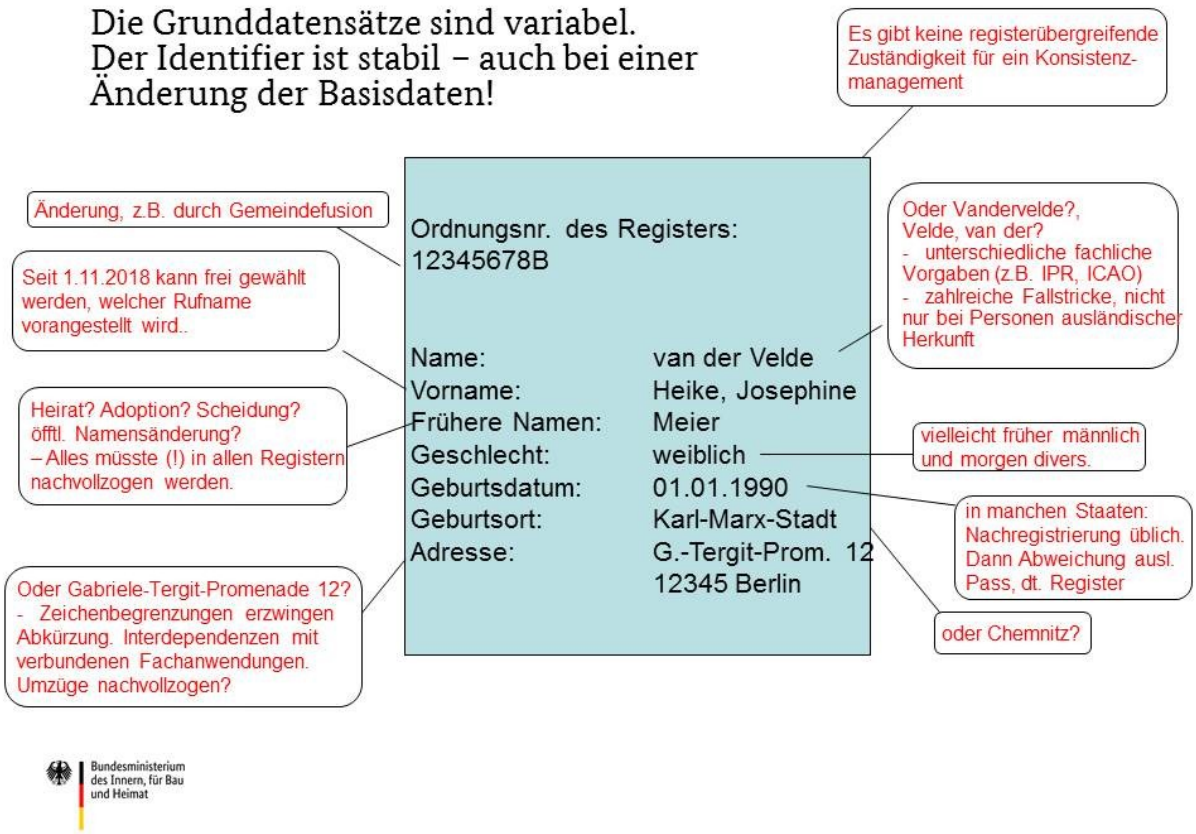
Mit dem registerübergreifenden Identitätsmanagement soll gewährleistet werden, dass sowohl die wahre Identität (Fragestellung: Führt die Person tatsächlich den Namen X und ist am Datum Y geboren?), als auch die Personalienidentität (Fragestellung: Beziehen sich zwei Datensätze auf dieselbe natürliche Person?) übereinstimmen und die aktuellen Basisdaten zur richtigen Person übermittelt werden können.

Als Basisdaten werden hier diejenigen personenbezogenen Daten bezeichnet, die ausschließlich zur korrekten Identifizierung einer Person dienen, insbesondere Vorname, Nachname, Geburtsdatum, Geburtsort, aktuelle Meldeadresse, Staatsangehörigkeit(en).

Oftmals wird von den „unveränderlichen Grunddaten einer Person“ gesprochen. Bei einer näheren Betrachtung der heutigen Lebenswirklichkeit stellen sich diese als überaus variabel dar. Bei Betrachtung der Grafik 2 wird dieses Problem anhand eines Beispieldatensatzes deutlich. Prinzipiell können sich alle Basisdaten ändern.

4.2 Verbesserungen durch einen numerischen Identifier

Im Gegensatz zu den veränderlichen Grunddatensätzen wie in Grafik 2 bleibt ein numerischer Identifier stabil - auch bei einer Änderung einzelner oder aller Basisdaten. Es gibt somit eine eindeutige Identifizierungsmöglichkeit, die über den Zeitverlauf erhalten bleibt.



Grafik 2: „Welche sind die unveränderlichen Grunddaten einer Person?“

Heute werden personenbezogene Basisdaten in einer Vielzahl dezentraler Register gespeichert – sowohl in der Innenverwaltung als auch den Bereichen Arbeit, Gesundheit, Justiz, Soziales etc. Die Aktualität und Validität kann dabei sehr unterschiedlich sein und ist z.B. abhängig davon, wann jeweils der letzte Verwaltungskontakt mit einem Bürger stattgefunden hat.

Zudem kann es aus fachlichen Gründen Abweichungen in der Darstellung der Daten geben, da z.B. Adressdaten für den Pass und Personalausweis und im Bereich des Meldewesens unterschiedlich gespeichert werden. Werden die Basisdaten dann zum Abgleich (anstatt eines numerischen Identifiers) für die behördeninterne Kommunikation benötigt, so müssen relativ große Datenkränze zu einer Person gespeichert und übermittelt werden, um diese Person möglichst eindeutig zu bestimmen. Dennoch gelingt dies, insbesondere in der digitalen Kommunikation, häufig nicht. Auf technischer Ebene führt dies typischerweise zu zwei Fehlersituationen:

- Es wird fälschlicherweise angenommen, dass zu einer Person noch keine Angaben im Register vorhanden sind (kein Treffer); oder

- ein automatisierter Prozess muss unterbrochen werden, weil Angaben zu mehreren Personen mit passenden Basisdaten gefunden wurden (mehr als ein Treffer).

Diese technischen Fehler können zu unterschiedlichsten fachlichen Fehlern führen, die von der Verwehrung staatlicher Leistungen trotz berechtigten Anspruchs über Leistungsmissbrauch bis zur Vortäuschung falscher Identitäten reichen.

Durch seine Variabilität ist der Grunddatensatz für die digitale Kommunikation zwischen Registern ein schlecht geeigneter Identifier. Sowohl hinsichtlich der Fehleranfälligkeit bei Übermittlungen, einer Pseudonymisierung für statistische Zwecke als auch der Datensparsamkeit bietet ein numerischer Identifier eindeutige Vorteile.

Die eindeutige Identifikation einer Person war und ist ein unverzichtbarer Grundpfeiler staatlichen Handelns. In der zunehmend digitalisierten Welt muss Eindeutigkeit sichergestellt werden, da es andernfalls zu Medienbrüchen (Prozessabbruch oder händisch auszuwertenden Trefferlisten) kommt.

Es muss der jeweils zutreffende Basisdatensatz einer Person korrekt referenziert werden können. Eine einmal erreichte Konsistenz („Diese 2 Datensätze betreffen dieselbe Person, obwohl die Angaben aus fachlichen Gründen ggf. nicht völlig identisch sind“) muss für zukünftige Sachverhalte erhalten bleiben.

Ein gleichbleibender numerischer Identifier kann diese Aufgaben zuverlässiger und datensparsamer erfüllen als der variable Grunddatensatz der Person. Der Identifier soll zumindest für die behördeninterne Kommunikation diese Eindeutigkeit sicherstellen und ermöglichen, dass bei einer Änderung in den Basisdaten einer Person durch die jeweils sachlich zuständige Behörde diese Änderung auch anderen Behörden zur Verfügung gestellt wird.

Neben den Aufgaben der Verbesserung des Identitätsmanagements (es werden die Daten zur richtigen Person übermittelt) und des Konsistenzmanagements (die Basisdaten einer Person sind in den Registern aktuell und identisch) leistet der Identifier auch einen Beitrag zur Stärkung der Interoperabilität von Registern, da über den gemeinsamen Identifier die Basisdaten einer Person verlässlich zugeordnet werden können.

Mit einem Identifier wäre es prinzipiell möglich, die Basisdaten einer Person aus den Fachregistern „auszulagern“ oder im Sinne der Datensparsamkeit zu reduzieren. Die Register könnten sich damit zukünftig auf das Führen ihrer jeweiligen Fachdaten, also der Daten, die über die personenbezogenen Basisdaten hinausgehen, konzentrieren.

Zudem leistet der Identifier einen wichtigen Beitrag zur Erreichung weiterer Ziele, z.B. einem registerbasierten Zensus oder der Erstellung amtlicher Statistiken aus vorhandenen Verwaltungsdaten, so dass eingriffsintensivere Maßnahmen vermieden werden können.

In einer - nicht vollumfänglichen - Aufzählung lassen sich die wichtigsten Verbesserungen eines Identifiers wie folgt zusammenfassen:

- ✓ Eineindeutige Zuordnung
- ✓ Keine Verwechslungen
- ✓ Keine Trefferlisten mit Daten Unbeteiligter
- ✓ Kein Abbruch digitalisierter E-Government-Prozesse, weil die korrekte Person nicht eindeutig referenziert werden konnte
- ✓ Vereinfachung der Digitalisierung von Verwaltungsleistungen
- ✓ Datensparsamkeit
- ✓ Konsistenzmanagement umsetzbar
- ✓ Interoperabilität der Register wird erleichtert
- ✓ Konzentration der Registerbehörde auf die Fachdaten
- ✓ Dezentrale Fachregister werden unterstützt
- ✓ Entlastung der Bürger von Nachweispflichten
- ✓ Leistungsgerechtigkeit
- ✓ Transparenz
- ✓ Wichtiger Baustein für Registerzensus
- ✓ Datenschutzfreundliche Pseudonymisierung möglich
- ✓ Bessere Nutzbarkeit vorhandener Verwaltungsdaten für amtliche Statistiken
- ✓ Abweichenden Namens- oder Adressschreibweisen aufgrund unterschiedlicher fachlicher Erfordernisse kann Rechnung getragen werden.

Für die Einführung eines Identifiers wurden Lösungen diskutiert, die in der Umsetzung relativ einfach (z.B. Nutzung eines vorhandenen Identifiers, hier der Steuer-ID) bis komplex sind (z.B. Rollout neuer Identifier über die Gesamtbevölkerung nebst kommunikativer Begleitung, ggf. ein verteiltes System mit Ver- und Entschlüsselung bei jedem bereichsübergreifenden Verwaltungskontakt, hier das später dargestellte bPK-Modell). Bei der Einrichtung eines Identifiers verlangen die verfassungs- und datenschutzrechtlichen Rahmenbedingungen - insbesondere das Volkszählungsurteil des BVerfG - besondere Aufmerksamkeit. Der bekannteste der bereits bestehenden Identifier in Deutschland ist die steuerliche Identifikationsnummer (Steuer-ID) nach § 139b der Abgabenordnung (AO).

4.3. Einrichtung eines Identitätsregisters mit Nutzung der Steuer-ID

Ein Identitätsregister wird benötigt, um eine registerübergreifend einheitliche Verantwortung für die Aktualität, Qualität und Konsistenz des Basisdatensatzes einer Person zu etablieren

und einen eindeutigen Identifier zu vergeben. Dies ist eine Aufgabe der Innenverwaltung, da alle der oben angeführten Basisdaten zur Identifizierung originär in der Innenverwaltung erhoben werden, z.B. in den Standesämtern, Meldebehörden und Ausländerbehörden.

Ein Identitätsregister, in dem die Basisdaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden, kann grundsätzlich durch den Ausbau bestehender Infrastrukturen oder durch den Aufbau einer neuen Datenbank errichtet werden. Es bestehen bereits heute Infrastrukturen, die für einen Ausbau grundsätzlich in Betracht kommen: Zum einen die Steuer-ID-Nummer-Datenbank des Bundeszentralamts für Steuern (BZSt) aus dem Finanzbereich und zum anderen die 15 Landesmelderegister der Innenverwaltung. Nordrhein-Westfalen benötigt kein Landesregister, weil es die derzeitigen Anforderungen zum Datenabruf über das sog. Meldeportal - mit dem alle Melderegister verknüpft sind – erfüllt. Die Stärke der 15 Landesmelderegister und der Portallösung in Nordrhein-Westfalen liegt jedoch in ihrer Funktion als Abrufregister. Für eine bundesweit übergreifende Qualitätssicherung und die Vergabe eindeutiger Identifier wären sie derzeit eher nicht prädestiniert und werden daher im Folgenden nicht weiter betrachtet.

Für die Vergabe eines Identifiers und eine übergreifende Qualitätssicherung der Identitätsdaten wurde vorrangig die Option einer Ausbaumöglichkeit des zentralen Registers beim BZSt geprüft. Für erforderliche Datenübermittlungen in oder aus anderen Registern kann das Meldewesen weiterhin seine Stärke als „informationelles Rückgrat der Verwaltung“ ausspielen. Insofern sind die Stärken beider Strukturen komplementär.

Die Steuer-ID-Datenbank des BZSt enthält keine Finanz- / Steuerdaten, sondern Daten, die der eindeutigen Identifikation einer Person dienen. In der Datenbank werden durch Datenübermittlungen der Meldebehörden alle meldepflichtigen Personen erfasst. Daten nicht meldepflichtiger, aber dennoch steuerpflichtiger Personen, werden teils von den Finanzämtern, teils durch das BZSt selbst erfasst. Unstimmigkeiten bei Datensätzen werden vom BZSt im Zusammenwirken mit den beteiligten Stellen (Finanzämter oder Meldebehörden) abgeklärt. Die Steuer-ID-Datenbank des BZSt spielt damit schon heute im Zusammenwirken mit den Meldebehörden eine wichtige Rolle bei der Qualitätssicherung der Daten in den Registern der Innenverwaltung.

Die Steuer-ID wird heute in vielen Behörden gespeichert, da sie für die Kommunikation mit den Finanzbehörden zu verwenden ist. Sie ist nach § 93c AO bei jeder gesetzlich vorgeschriebenen Mitteilung an die Finanzbehörden anzugeben. Die Verwendung der Steuer-ID ist heute auf den steuerlichen Bereich beschränkt. Gleichwohl wird die Steuer-ID dabei auf rechtlicher Grundlage in einer Vielzahl von Registern gespeichert, weshalb sie sich als Identifier für ein registerübergreifendes Identitätsmanagement besonders eignet. Hier hat der

kosten- und zeitintensive Roll-out in Fachverfahren und Registern verschiedener Bereiche - nicht nur der Finanzverwaltung - bereits stattgefunden:

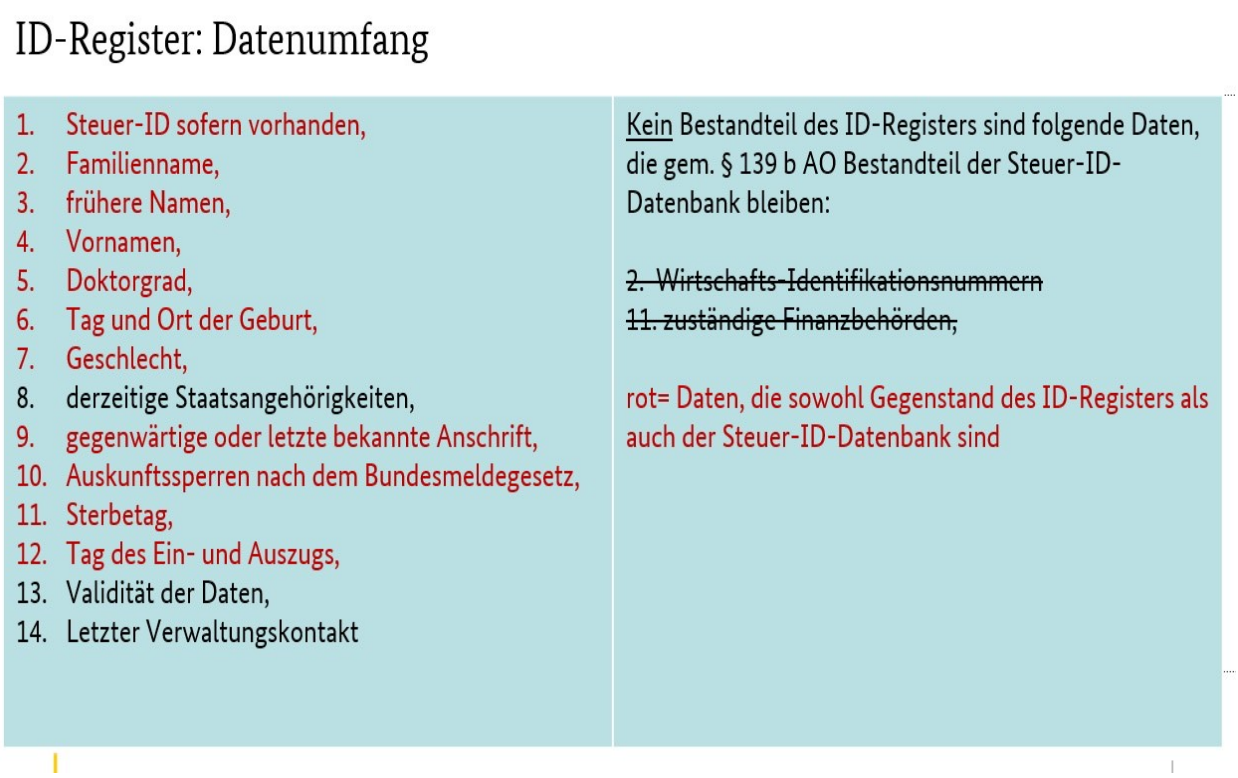
- ✓ Meldebehörden nach § 3 Abs. 2 Nr. 2d Bundesmeldegesetz
- ✓ Deutsche Rentenversicherung sowie private Versicherungen im Rahmen des Rentenbezugsmitteilungsverfahrens (RBM-Verfahren, ca. 36 Mio. RBM, pro Rente eine RBM, ca. 1,6 Renten pro Person) nach § 22a EStG.
- ✓ Lohnersatzleistungen, z.B. Insolvenzgeld, Elterngeld, Arbeitslosengeld etc. nach § 32b EStG.
- ✓ Arbeitgeber im Rahmen des Lohnsteuerabzugsverfahren (ELStAM) mit IdNr. für ca. 40 Mio. Arbeitnehmer nach § 39e EStG.
- ✓ Banken nach § 154 Abs. 2a AO, Kirchensteuer aus Kapitalerträge (KiStAM) nach § 51 Abs. 2c EStG, Freistellungsauftrag nach § 45d EStG), IdNr. für jeden Kontoinhaber, Verfügungsberechtigten oder wirtschaftlich Berechtigten
- ✓ Gerichte und Notare nach §§ 18, 20 Abs. 1 Nr. 1 GrEStG, 34 ErbStG, 7 Abs. 2 Nr. 1 und Abs. 3 Nr. 3 ErbStDV

Während die Qualitätssicherung in allen dezentralen Fachregistern in unterschiedlichen fachlichen Ausprägungen – und stets abhängig von den vorhandenen Personalressourcen – ausgeführt werden, bietet sich ein zentrales Identitätsregister für gezielte Qualitätssicherungsmaßnahmen über den Gesamtdatenbestand an. Hier knüpft auch die Erfahrung aus der Praxis an, dass eine Identität, sofern sie einmal behördlich akzeptiert wurde, in der Folge häufig nicht mehr geprüft wird, obwohl an anderer behördlicher Stelle neue Erkenntnisse bestehen. So besteht die Gefahr, dass sich Falschidentitäten verfestigen. Ein zentrales Register kann dazu beitragen, die behördliche Zusammenarbeit im Hinblick auf die Personenbasisdaten im Rahmen von Qualitätssicherungsaufgaben, z.B. Dublettenläufen, zu verbessern.

4.4 Datenumfang und Qualitätssicherung im Identitätsregister

Datenkranz, Personenkreis und Aufgaben der Steuer-ID-Datenbank des BZSt weisen bereits jetzt einen hohen Deckungsgrad zu den Anforderungen der IMK auf. Hervorzuheben ist vor allem die große Expertise des BZSt im Bereich der Vergabe eindeutiger Identifikatoren und der Qualitätssicherung von Identitätsdaten. Die wahre Identität von Personen wird allerdings durch die Steuer-ID-Datenbank bisher nicht hinterfragt.

Das Ergebnis der fachlichen Arbeit auf Arbeitsebene und in den Expertengruppen bei der Ermittlung des zukünftigen fachlich erforderlichen Datenumfangs eines Identitätsregisters zeigt die folgende Grafik 3.



Grafik 3: Datenumfang des Identitätsregisters in Abgrenzung zum Datenumfang der heutigen ID-Nummer-Datenbank im Bundeszentralamt für Steuern.

Danach kann auf dem heutigen Datenumfang der Steuer-ID-Datenbank nach § 139b Abs. 3 AO grundsätzlich aufgebaut werden. Die Datenfelder „Wirtschafts-Identifikationsnummer“ und „zuständige Finanzbehörden“ sind für das registerübergreifende Identitätsmanagement nicht erforderlich. Daher könnte eine Realisierung des Identitätsregisters sehr datensparsam, ressourcenschonend und schnell umgesetzt werden, indem anstatt der Einrichtung eines neuen Registers oder einer Spiegeldatenbank zukünftig lediglich die Sichten auf die bestehende ID-Nummer-Datenbank durch ein neues Rechte- und Rollenkonzept angepasst werden. Derart würde die Sicht auf die Datenbank für die Finanzverwaltung unverändert erhalten bleiben, die Sicht der identitätsregisternutzenden Stellen jedoch die beiden oben genannten Datenfelder auslassen, und dafür aus dem fachlichen Bedarf heraus drei neue Datenfelder der bestehenden Datenbank hinzugefügt werden: „derzeitige Staatsangehörigkeiten“, ein Wert für die „Validität der Daten“ im Identitätsregister und mit dem Wert „letzter Verwaltungskontakt“ ein Hinweis darauf, wann ein Bürger – zumindest was die an das Identitätsregister mittel- und unmittelbar angeschlossenen Fachverfahren und Register anbelangt – das letzte Mal persönlichen Kontakt mit der öffentlichen Verwaltung hatte. Diese neu einzurichtenden Datenfelder sollen im Folgenden besser vorgestellt werden.

4.4.1 Neues Datenfeld Validität

Der Wert im neuen Datenfeld Validität meint die Verlässlichkeit, mit der die Übereinstimmung eines Personenbasisdatensatzes im Identitätsregister mit den wahren personenidentifizierenden Basisdaten einer Person angenommen werden kann. Die Ermittlung der Validität der im Identitätsregister erfassten Angaben soll u.a. auf Basis der im Melderegister gespeicherten Hinweise[1] auf die der Erfassung des jeweiligen Attributwertes zu Grunde liegenden Nachweise erfolgen. Die Hinweise dienen der Identifizierung des Nachweises und werden bei dessen Vorlage im Rahmen der Eintragung, z.B. im Melderegister, erfasst.

Für die Darstellung der Validität sollen drei Werte gebildet werden:
Wert 1: Für alle in die Validierung einbezogenen Angaben im Identitätsregister sind im Melderegister Hinweise eingetragen (voraussichtlich für alle in Deutschland geborene deutsche Staatsangehörige der Fall).
Wert 2: Für einige der in die Validierung einbezogenen Angaben im Identitätsregister sind im Melderegister Hinweise eingetragen.
Wert 3: Für keine der in die Validierung einbezogenen Angaben im ID-Register sind im Melderegister Hinweise eingetragen.

Ein Wert 3 könnte z.B. beinhalten, dass die vorhandenen Personenbasisdaten aufgrund nicht vorhandener Dokumente „auf eigenen Angaben“ einer Person beruhen. Dieser Sachverhalt wird in den Registern gegenwärtig unterschiedlich abgebildet. Im AZR unterbleibt ein solcher Hinweis, wird jedoch auf dem Ankunftsnachweis (Bescheinigung über die Meldung als Asylsuchender) dokumentiert[2].

Die Angabe der Validität unterstützt Datenempfänger bei der Entscheidung, ob die anstehende Verwaltungsleistung auf Basis der vorliegenden Angaben erbracht werden kann. Die elektronische Verfügbarkeit dieser Information trägt zu einem medienbruchfreien Verwaltungshandeln bei. Die Hinweise selbst werden dabei im Identitätsregister nicht gespeichert und können u.a. aus dem Melderegister abgerufen werden. Damit wird gewährleistet, dass der Charakter des Identitätsregisters als Datenbank ausschließlich zu Identitätsdaten erhalten bleibt.

[1] Zum Begriff des „Hinweises“ im Meldewesen: Hinweise sind die im Melderegister gemäß dem Datensatz für das Meldewesen gespeicherten weiteren Angaben hinsichtlich der Art der Daten, deren Herkunft und Ausstellungs- bzw. Gültigkeitsdatum.

[2] Ankreuzbar ist das Feld „Die Angaben zur Person beruhen auf den eigenen Angaben der Inhaberin/des Inhabers. Ein Identifikationsnachweis durch Originaldokumente wurde nicht erbracht. Die Inhaberin/der Inhaber genügt mit dieser Bescheinigung nicht der Pass- und Ausweispflicht.“

„Eigentümer“ dieser Daten, in dessen Verantwortung die Aktualität der Angabe und ggf. auch die Aktualität der Zuordnung des Datensatzes liegt, sind z.B. das AZR[3], Meldebehörden etc.

4.4.2 Neues Datenfeld Letzter Verwaltungskontakt (Lebenszeichenansatz)

Die Qualität der Daten im Identitätsregister hängt nicht nur von der Arbeitsweise in den zuliefernden Behörden, sondern auch von der Mitwirkung der Bürgerinnen und Bürger ab. Durch wechselnde Lebenslagen sind deren Daten ständig von Veränderungen betroffen, so dass eine gute Datenqualität Arbeitsgegenstand und Ziel eines kontinuierlichen Prozesses der Qualitätssicherung im Identitätsregister ist. Nach den Vorstellungen des Lebenszeichenansatzes könnte das Datenfeld „Letzter Verwaltungskontakt“ „eingeschaltet“ werden, wenn für einen Bürger in einem (der fachlich noch festzulegenden) Vergleichsregister eine Aktivität in einem definierten Zeitraum stattgefunden hat.

Ein - fachlich von der Expertengruppe 3 noch nicht finalisiertes - Szenario der Nutzung sieht bspw. so aus, dass aus festzulegenden Vergleichsregistern bei zu bestimmenden Anlässen das Lebenszeichen-Datenfeld eingeschaltet wird. Unterbleibt ein Einschalten in einem definierten Prüfzeitraum, kann dies ein Hinweis darauf sein, dass es sich bei dem Datensatz im Identitätsregister um eine Dublette handelt. In diesem Fall könnte die identitätsregisterführende Stelle eine Bitte auf Prüfung der Richtigkeit und ggf. Fortschreibung veranlassen.

Die Anforderungen des Datenschutzes an ein Datenfeld „Letzter Verwaltungskontakt“ sind dabei zu berücksichtigen. Dies könnte u.a. dadurch erfolgen, dass dieses Datenfeld als Wahrheitswert, als ungenaue Datumsangabe aus Monat und Jahr oder als Zähler ausgestaltet wird, der bei Kontakten zu Vergleichsregistern in einem definierten Zeitraum hochgezählt und wieder reduziert wird, wenn ein Kontakt außerhalb des relevanten Prüfzeitraums liegt. Angaben, bei welchem Vergleichsregister das Lebenszeichen entstanden ist, würden im Identitätsregister nicht gespeichert.

Der Mehrwert für die Verwaltung bestünde in der Möglichkeit der kontinuierlichen Pflege der Datenbestände, der Verbesserung der Datenqualität und Bereitstellung eines gepflegten Personenbasisdatenbestandes für alle Verwaltungsprozesse.

[3] Welche Daten an die Registerbehörde zu übermitteln und von dieser zu speichern oder – falls erforderlich – zu berichtigen oder zu aktualisieren sind, können nur die Stellen wissen, bei denen die Daten anfallen oder die zu ihrer Übermittlung an das AZR verpflichtet sind. Sie allein verfügen über die erforderliche Sachnähe. Insofern haben in erster Linie die Ausländerbehörden – und in Asylangelegenheiten das BAMF – die Verpflichtung, Daten an das AZR zu übermitteln, die übermittelten Daten zu prüfen und ggf. zu aktualisieren.

4.4.3 Neues Datenfeld Staatsangehörigkeiten

Während die Speicherung eines Datenfelds „Staatsangehörigkeiten“ für die Finanzverwaltung nicht erforderlich und damit in § 139b Abs.3 AO nicht enthalten ist, wird dieses Datenfeld in der Innenverwaltung und in vielen anderen Verwaltungsbereichen als wichtiges Basisdatum betrachtet, das eine wesentliche Aussage über die Identität der Person trifft und für die Verwaltungsarbeit ständig gebraucht wird.

Identität und Staatsangehörigkeit sind in staatsangehörigkeitsrechtlichen Angelegenheiten wesentliche Daten, ohne die der Erwerb und Verlust der deutschen Staatsangehörigkeit nicht ohne Weiteres festgestellt werden kann. So sind die geklärte Identität und Staatsangehörigkeit für die Einbürgerung gesetzliche Tatbestandsvoraussetzung. Sie gehören zusammen, da sich ohne diese auch nicht die übrigen Einbürgerungsvoraussetzungen prüfen lassen, u.a. ob der Betroffene im In- oder Ausland eine Straftat begangen hat.

Für die Qualitätssicherungsmaßnahmen, insbesondere für eine Dublettenprüfung, wird das Datenfeld Staatsangehörigkeiten einen wichtigen Beitrag beisteuern.

5. Gewährleistung Verfassungsrecht, Datenschutz und Transparenz

5.1 Vorbemerkung

Eine umfassende verfassungs- und datenschutzrechtliche Würdigung des registerübergreifenden Identitätsmanagements ist an dieser Stelle nicht möglich. Es wurden auf Arbeitsebene und in den Sitzungen der Expertengruppen zahlreiche verfassungs- und datenschutzrechtliche Fragestellungen erörtert. Auch weil sich seit dem Urteil des BVerfG zur Volkszählung die technischen, rechtlichen und gesellschaftlichen Rahmenbedingungen verändert haben, ist ungewiss, wie das Recht auf informationelle Selbstbestimmung vom BVerfG in einen der fortentwickelten Informationstechnik entsprechenden Kontext gestellt würde. Dies zeigt beispielsweise die Bewertung eines registerbasierten Zensus, den das BVerfG im Volkszählungsurteil 1983 (BVerfGE 65, 1 ff) noch verworfen, im Zensusurteil 2018 (BVerfG, Urteil des Zweiten Senats vom 19. September 2018, Az. 2 BvF 1/15) jedoch als im Verhältnis zur Direkterhebung grundrechtsschonendere Variante benannt hat.

5.2 Gewährleistung Verfassungsrecht, Datenschutz und Transparenz

Die angestrebte Gestaltung und Änderung der Registerlandschaft im Hinblick auf die Einführung eines registerübergreifenden Identitätsmanagements erfordern zunächst eine verfassungsrechtliche Bewertung, insbesondere in Bezug auf die Frage, ob ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Bürger zu rechtfertigen ist.

Leitend für die Konzeption und Umsetzung sind dabei insbesondere Rechtmäßigkeit, Zweckbindung, Datensparsamkeit und Datensicherheit als Grundsätze für die Verarbeitung personenbezogener Daten. Nach der Rechtsprechung des BVerfG ist im Hinblick auf das informationelle Selbstbestimmungsrecht insbesondere darauf zu achten, dass eine Zusammenführung aller mit dem Kennzeichen verbundenen Daten und damit die Herstellung von Persönlichkeitsprofilen („Gesamtbild der Persönlichkeit“) durch organisatorische, technische und rechtliche Maßnahmen wirksam verhindert wird. Ferner ist begründet darzulegen, dass unter Berücksichtigung der verfolgten Ziele der Grundrechtseingriff im Ergebnis verhältnismäßig ist, wobei u.a. die in dem Urteil des BFH, Urteil vom 18.01.2012 (Az. II R 49/10) zur Steuer-ID genannten Kriterien heranzuziehen sind. Hiernach ist die Eingriffstiefe umso geringer, je weniger der Identifier selbst Persönlichkeitsrelevanz aufweist, Datenerhebungen weder heimlich noch unter gesteigerten Mitwirkungspflichten erfolgen oder besondere Vertraulichkeitserwartungen verletzt werden.

Bei einer verfassungsgemäßen Konzeption für die Umsetzung des Identitätsmanagements ist die Gewährleistung des Datenschutzes durch die Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen sicherzustellen, um den mit der Datenverarbeitung einhergehenden Risiken zu begegnen. Die rechtlichen Rahmenbedingungen finden sich dazu in der DSGVO und ggf. ergänzenden Regelungen. Die DSGVO lässt in Artikel 87 Kennzeichen von allgemeiner Bedeutung zu. Die zur Risikominimierung erforderlichen Abhilfemaßnahmen sollten dabei bereits bei der Konzeption – ebenso wie bei der Erstellung der erforderlichen Rechtsgrundlagen – durch geeignete Weichenstellungen und Voreinstellungen gemäß den Vorgaben des Artikel 25 DSGVO („Privacy by Design“) berücksichtigt werden, sodass technische und organisatorische Maßnahmen bereits in die Grundkonzeption einfließen, um die datenschutzrechtlichen Anforderungen wirksam umzusetzen.

Daher wurde auf Arbeitsebene und in den Expertengruppen einvernehmlich anerkannt, dass mit der Einführung eines Identifiers aus verfassungs- und datenschutzrechtlichen Gründen Maßnahmen zu ergreifen sind, die wirksam verhindern, dass es durch eine unzulässige Zusammenführung einzelner Personenbasisdaten mit den zugehörigen Fachdaten in den dezentralen Registern zur Erstellung eines umfassenden Persönlichkeitsprofils kommen kann. Beide Modelle, die im Kapitel 6 über das Basismodell hinausgehen, folgen dieser Auffassung, auch wenn sie der Gefahr einer unrechtmäßigen Datenzusammenführung in unterschiedlicher Ausprägung begegnen. Einigkeit konnte darüber hergestellt werden, dass trotz der datenschutzrechtlichen Sicherungsmaßnahmen zugleich sichergestellt sein muss, dass rechtmäßige Datenübermittlungen effizient möglich sind und zuverlässig funktionieren. Für jede Datenübermittlung bedarf es einer entsprechenden Rechtsgrundlage. In der nach dem

Prinzip der behördlichen Zuständigkeit dezentral organisierten Registerlandschaft der öffentlichen Verwaltung ist die Zusammenführung von Daten gleichbedeutend mit der Übermittlung von Daten. Daher soll die unzulässige Zusammenführung einzelner Lebens- und Personaldaten, die zur Erstellung von Persönlichkeitsprofilen führen könnte, dadurch ausgeschlossen werden, dass Kontrolle über Datenübermittlungen zwischen Behörden ausgeübt wird.

Ein Blick auf die vorgenannten Urteile des BVerfG und BFH erlaubt zusätzliche Erkenntnisse im Hinblick auf das registerübergreifende Identitätsmanagement: so wurde bspw. im vorgenannten BFH-Urteil zur bisherigen Ausgestaltung der Steuer-ID als bereichsspezifischem Identifikator festgestellt, dass die Zuteilung der Identifikationsnummer und die dazu erfolgte Datenspeicherung mit dem Recht auf informationelle Selbstbestimmung und sonstigem Verfassungsrecht vereinbar sind. Die in dem Urteil aufgestellten Grundsätze geben Hinweise für die Gestaltung des registerübergreifenden Identitätsmanagements. Die Behörden müssen aufgrund ihrer gesetzlichen Befugnisse in der Lage sein, Personenbasisdaten in mehreren Registern der Verwaltung aufgrund einer rechtlichen Vorschrift korrekt zuordnen zu können. Ebenso müssen sie aus hiesiger Sicht organisatorisch und technisch fähig sein, die gebotenen Zuordnungen durch die behördeninterne Verwendung der Steuer-ID auch effizient vorzunehmen. Im obigen Urteil wurde im Übrigen zu den mit der Einführung der Steuer-ID verfolgten Ziele (Bürokratieabbau innerhalb und außerhalb der Verwaltung, Gleichmäßigkeit der Besteuerung) festgestellt, dass sie nicht gegen das Recht auf informationelle Selbstbestimmung oder sonstiges Verfassungsrecht verstoßen. Das registerübergreifende Identitätsmanagement dient mehreren legitimen Zwecken:

- Die eindeutige Zuordnung auch im digitalen Verwaltungshandeln dient der Leistungsgerechtigkeit staatlichen Handelns.
- Indem in der Verwaltung vorhandene Nachweisdaten durch Datenübermittlung zwischen Behörden für die Vorbereitung einer Verwaltungsleistung herangezogen werden können, werden Bürgerinnen und Bürger von Nachweispflichten entlastet. Dies erleichtert insbesondere sozial schwächeren oder im Umgang mit der Verwaltung wenig versierten Bürgerinnen und Bürgern die Geltendmachung ihrer Ansprüche.
- Es wird Leistungsmissbrauch durch den Gebrauch von Falschidentitäten vorgebeugt.
- Stets soll mit dem Zweck der Zuordnung von Datensätzen in unterschiedlichen Registern aufgrund einer rechtlichen Grundlage durch die Steuer-ID ein korrektes Verwaltungshandeln ermöglicht werden.

Wie bei der heutigen Verwendung der Steuer-ID durch die Finanzverwaltung sollen auch nach Einführung des registerübergreifenden Identitätsmanagements Bescheide der Verwaltung unter dem Namen des jeweiligen Bürgers bekannt gegeben und auch zukünftig z.B. der

Personalausweis verwendet werden, um sich vor der Verwaltung auszuweisen. Die Steuer-ID dient im registerübergreifenden Identitätsmanagement lediglich als ein behördeninternes Ordnungsmerkmal. Die Bürgerinnen und Bürger werden dadurch nicht zum Objekt gemacht. Die Behörden der öffentlichen Verwaltung werden die Steuer-ID nur erheben und verwenden können, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Steuer-ID ausdrücklich erlaubt oder anordnet.

Im Gegenteil sorgt die Verwendung der Steuer-ID dafür, dass bei der Datenübermittlung auf rechtlicher Grundlage nicht umfassende „sprechende“ Personenbasisdaten ausgetauscht werden müssen und trägt insofern zum Grundsatz der Datensparsamkeit bei. Die Verwendung der Steuer-ID ermöglicht ebenso, dass sich die dezentralen Fachregister auf das Führen der erforderlichen Fachdaten statt auf die Speicherung personenidentifizierender Basisdaten konzentrieren können.

Die deutliche Erhöhung der Effizienz der Verwaltung durch das registerübergreifende Identitätsmanagement ist ein bedeutsamer zusätzlicher Faktor. Diese Potentiale müssen gleichwohl aus dem Gebot der Wirtschaftlichkeit des Verwaltungshandelns gehoben werden.

Der IMK-Beschluss beinhaltet auch die Anforderung, dass die betroffenen Bürgerinnen und Bürger im Rahmen ihres datenschutzrechtlichen Auskunftsrechts jederzeit auf einfache Weise feststellen können, welche Behörde zu welchem Zweck auf welche ihrer Daten zugegriffen hat. Diese Transparenz kann im Sinne des Volkszählungsurteils des BVerfG zugleich freiheitsschützende Wirkung entfalten, indem die tatsächlichen Möglichkeiten der betroffenen Person, die Richtigkeit und Verwendung ihrer Daten zu kontrollieren, entscheidend verbessert werden. Auch hierfür schafft das registerübergreifende Identitätsmanagement die infrastrukturellen Voraussetzungen. Das Recht auf informationelle Selbstbestimmung kann gestärkt und der verfahrensrechtliche Grundsatz der Waffengleichheit durch die geplante Bereitstellung eines „Datencockpits“ (DC) und der damit erleichterten Wahrnehmung datenschutzrechtlicher Auskunftsrechte gefördert werden.

Das gegenwärtig im Rahmen der OZG-Umsetzung konzipierte Datencockpit soll es für Bürger nachvollziehbar machen, welche (Meta-) Daten zu welchem Zweck zwischen welchen Behörden ausgetauscht worden sind. Dieses Transparenzversprechen soll zum einen Bürger dazu ermutigen, dem automatisierten Datenaustausch zwischen Behörden im Rahmen von Online-Verwaltungsprozessen (z.B. der Zustimmung zum automatisierten Austausch der Daten zur Geburtsurkunde bei der Beantragung Elterngeld) zuzustimmen und damit die Nutzerfreundlichkeit dieser Prozesse zu verbessern. Zum anderen kann hierdurch eine nutzer-

freundliche Möglichkeit zur Wahrnehmung der datenschutzrechtlichen Auskunftsrechte bereitgestellt werden. Eine solche Komponente wäre im Verantwortungsbereich des IT-Planungsrates, etwa im Zusammenhang mit der OZG-Infrastruktur, z.B. über Nutzerkonten im Portalverbund, zu realisieren. Aus Sicht des IMK-Vorhabens für ein registerübergreifendes Identitätsmanagement wird die Realisierung eines DC für die Akzeptanz des Identitätsmanagements befürwortet. Für Bürger, die aus dem Ausland Verwaltungskontakt mit einer deutschen Behörde haben, sollte ebenfalls ein Nutzerkonto im Portalverbund mit Zugang zu einem Datencockpit bereitgestellt werden.

6. Modellauswahl für die Zielarchitektur

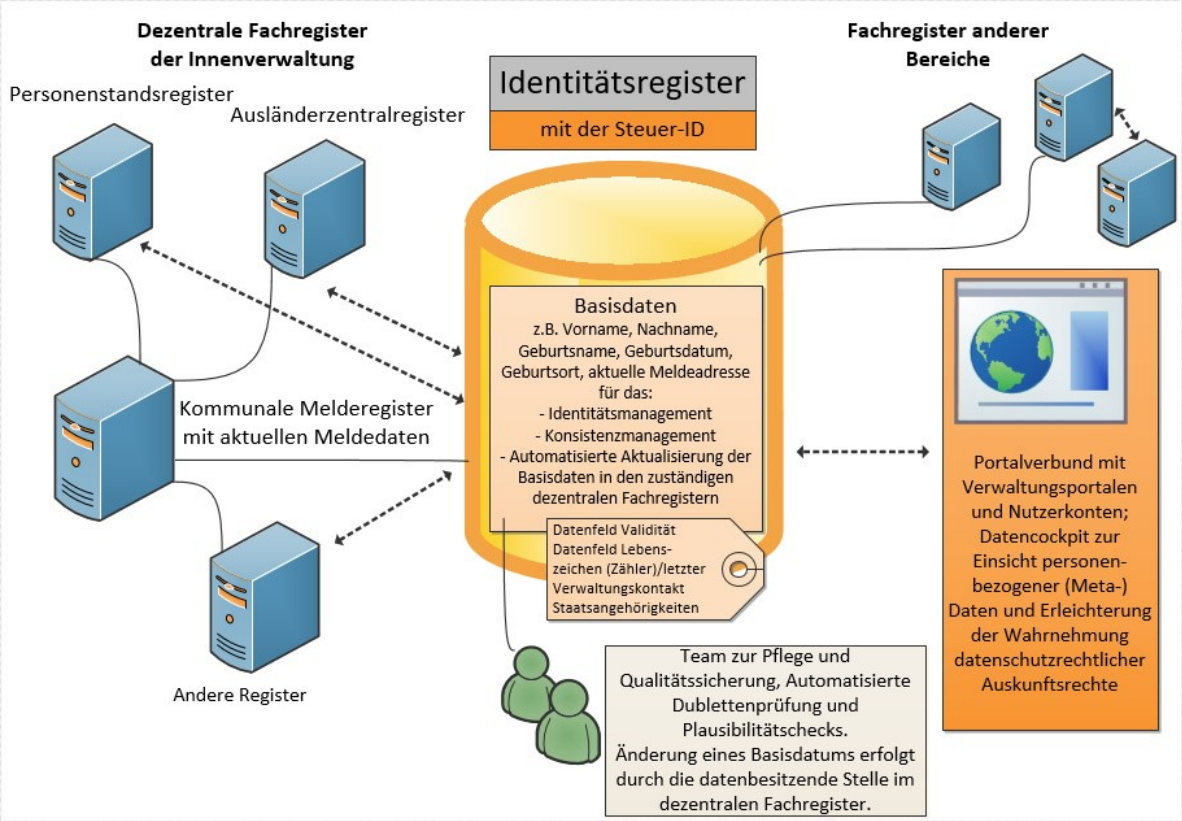
Im Folgenden sollen drei Modelle dargestellt werden, die als Lösungsvarianten für das registerübergreifende Identitätsmanagement auf Arbeitsebene diskutiert wurden. Dabei ist das nachfolgend beschriebene Basismodell in der weiteren Diskussion durch zwei Modelle mit erhöhten verfassungs- und datenschutzrechtlichen Sicherungen ergänzt worden.

6.1 Basismodell

Das Basismodell ist das einfachste, das aus fachlicher Sicht die Anforderungen der IMK erfüllen würde. Die Aufgabenbeschreibung des Identitätsregisters im Basismodell sieht vor:

- ✓ an jede natürliche Person, die Beteiligte eines Verwaltungsverfahrens einer inländischen öffentlichen Stelle ist, zum Zwecke der eindeutigen Zuordnung in den Datenbeständen der öffentlichen Verwaltung einen Identifier zu vergeben,
- ✓ die Basisdaten zur Person stets aktuell und in hoher Qualität bereitzuhalten und inländischen öffentlichen Stellen für die Erfüllung ihrer Aufgaben zur Verfügung zu stellen,
- ✓ Qualitätssicherungsprozesse zu initiieren und zu koordinieren, um in Kooperation mit anderen öffentlichen Stellen die Aktualität, Validität und Konsistenz der Grunddaten sicherzustellen.

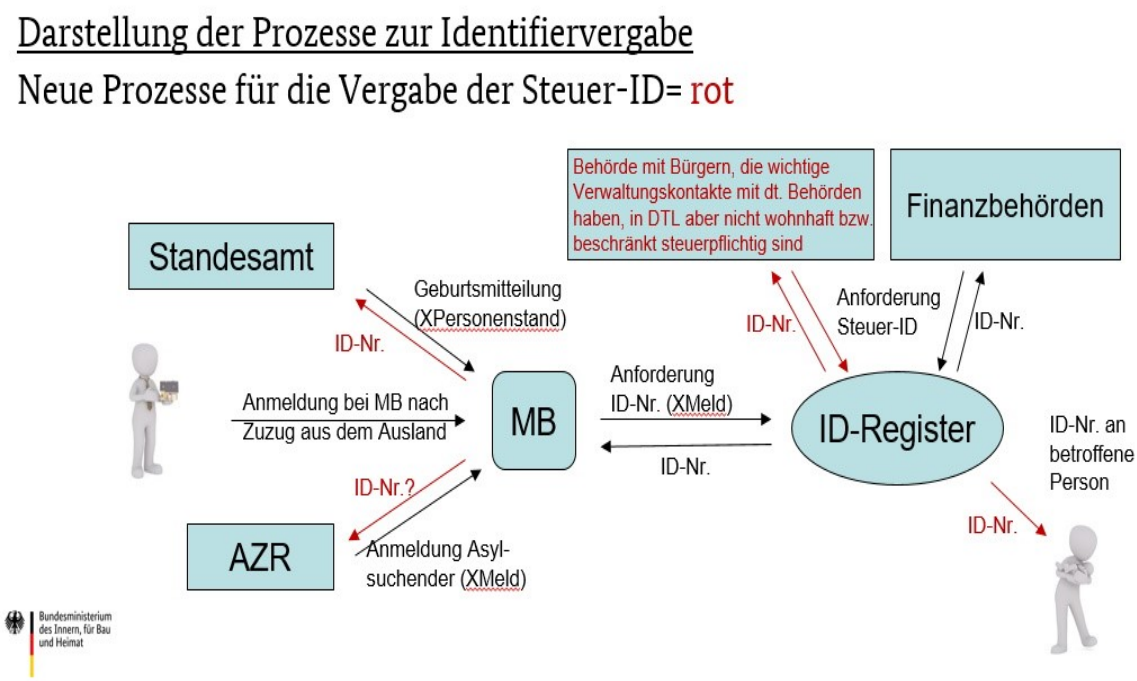
Das Basismodell (Grafik 4) sieht vor, die Steuer-ID als einzigen Identifier zukünftig in den Registern der öffentlichen Verwaltung den jeweiligen Personendaten zuzuspeichern.



Grafik 4: Basismodell eines registerübergreifenden Identitätsmanagements mit der Steuer-ID als numerischem Identifier. Durchgezogene Linien stehen für bestehenden Datenaustausch, gestrichelte Linien für eine denkbare zukünftige Datenaustauschbeziehung. Fachregister können auch mittelbar an das Identitätsregister angebunden werden.

Im Bereich der Innenverwaltung können dabei für den Roll-out und die Datenübermittlungen des laufenden Betriebs die bestehenden Prozesse mit geringfügigen Ergänzungen weiter genutzt werden. Erneut kommt hier dem Meldewesen eine bedeutende Rolle als Verteilstelle der Daten in Zusammenarbeit mit der ID-Nummer-Datenbank des BZSt zu (Grafik 5). In dieser Grafik sind die möglichen neuen Prozesse zur Vergabe der Steuer-ID mit Rot gekennzeichnet.

Die Grafik verdeutlicht, dass aufgrund der bestehenden Infrastruktur ein Roll-out des neuen Identifiers - der Steuer-ID - sehr effizient vorgenommen werden kann und der Aufbau einer neuen „sternförmigen Kommunikationsstruktur“ zum Identitätsregister nicht erforderlich ist.



Grafik 5: Darstellung der Prozesse zur Vergabe des Identifiers.

Zusätzlich wird allen öffentlichen Stellen das heute bereits eingesetzte maschinelle Abfrageverfahren (MAV) im BZSt angeboten, so dass bei Vorhandensein der Steuer-ID mit Angabe des Geburtsdatums die Basisdaten der zugehörigen Person vom Identitätsregister übermittelt werden bzw. umgekehrt bei der Angabe vorhandener Basisdaten zu einer Person im Ergebnis die Steuer-ID dieser Person vom Identitätsregister übermittelt wird. Sofern eine Rechtsvorschrift zur Erhebung oder Übermittlung von Daten zwischen öffentlichen Stellen besteht, darf dann auch die Steuer-ID zum Zweck der eindeutigen Zuordnung der Daten zu einem Bürger verwendet werden.

Das Basismodell sieht Vorschriften zur Protokollierung, Löschung und Sanktionen für Datenschutzverstöße nach DSGVO bzw. zu persönlichem Fehlverhalten nach §§ 41 bis 43 BDSG vor. Es geht von der Annahme aus, dass die bestehenden Datenaustauschbeziehungen der öffentlichen Verwaltung verfassungs- und datenschutzkonform erfolgen und die Übermittlung der Steuer-ID anstelle der Personenbasisdaten als Identifier keine grundlegend andere Situation schafft. Es sieht nach dem Verständnis insbesondere der Datenschutzbeauftragten grundsätzlich keine zusätzlichen im Modell eingebauten datenschutzrechtlichen Sicherungsmechanismen (in der Diktion der Datenschutzbeauftragten: „strukturelle Hemmnisse“) vor, die greifen, weil angenommen werden müsse, dass die Verwendung eines gegenüber dem Personenbasisdatensatz zuverlässigeren numerischen Identifiers eine Kompensation dieser

erhöhten Effektivität erfordere, um eine vollständige Zusammenführung und Katalogisierung von Personendaten zu verhindern.

Die beiden folgenden Modelle, die in den Expertengruppen erörtert wurden, beinhalten solche Sicherungsmechanismen. Beide Modelle sollen zunächst ohne eine Bewertung dargestellt werden, für einen weitergehenden Überblick sind sie in der separaten Anlage zu finden.

6.2 Modell mit mehreren bereichsspezifischen Identifikatoren

Im Anschluss an die ersten gemeinsamen Sitzungen der Expertengruppen „Registerarchitektur" und „Identifier" wurde im Dezember 2019 ein Modell für die Verwendung bereichsspezifischer Personenkennzeichen (bPK) für Deutschland konkretisiert und in der folgenden gemeinsamen Sitzung am 14./15. Januar 2020 vorgestellt (Anlage). Die erarbeiteten Vorschläge mit Verwendung bereichsspezifischer Personenkennzeichen gehen ebenfalls von einem zentralen Identitätsregister aus, das folgende Aufgaben zugewiesen bekommt:

- Berechnung der Stammzahl aus der Steuer-ID und der daraus abgeleiteten bPKs.
- Bereitstellung der bPKs auf Anfrage an einen Berechtigten.
- Bereitstellung eines verschlüsselten bereichsfremden bPK (oder einer alternativen Methode) an einen Berechtigten zur Kommunikation mit einer Behörde eines anderen Bereichs.
- Abruf von Daten aus dem Datenkranz des Identitätsregisters durch alle berechtigten Stellen unter Angabe des bPK.

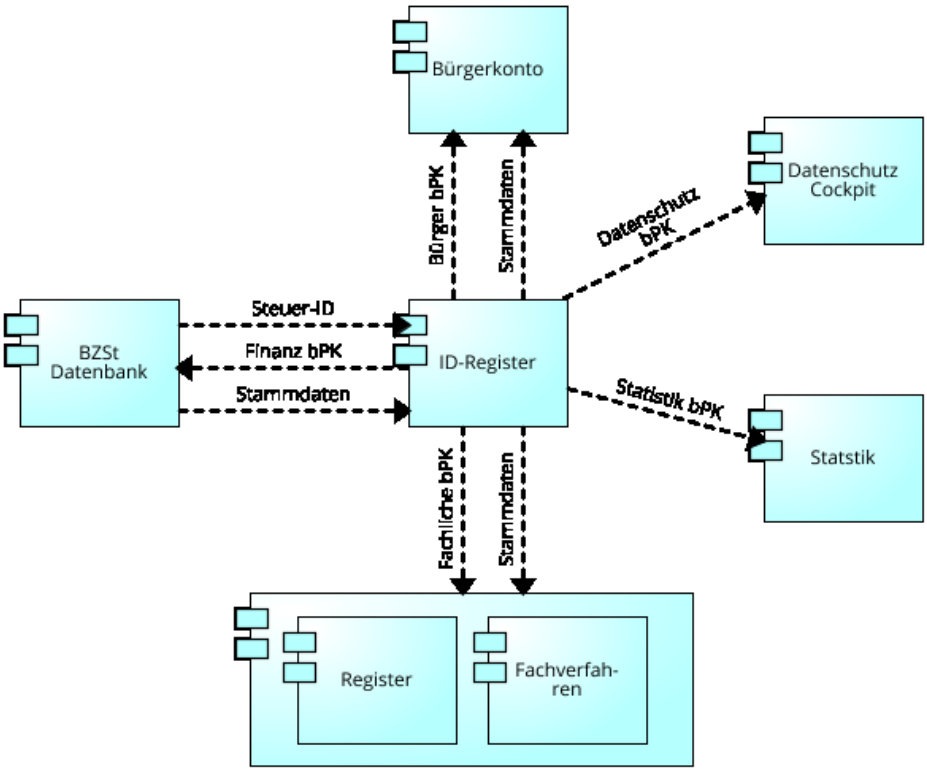
Weitere Merkmale des vorgestellten Modells sind:

- Der Datenaustausch erfolgt mittels verschlüsselter bereichsfremder bPKs. Das neu zu errichtende Identitätsregister stellt einer berechtigten anfragenden Behörde das gewünschte bereichsfremde bPK bereit, welches mittels des öffentlichen Schlüssels der Zielbehörde für den Datenaustausch verschlüsselt wird. So kann nur die Zielbehörde das bPK entschlüsseln.
- Nach dem initialen Abruf des verschlüsselten bPK des Fremdbereichs könnte eine weitere Kommunikation mit dem Identitätsregister entfallen, falls das betreffende bPK jeweils bei den Kommunikationspartnern gespeichert werden könnte. Sofern eine Zuspeicherung der Fremd-bPK im jeweiligen Fachregister nicht vorgenommen werden soll, muss die Kommunikation bei jedem bereichsfremden Verwaltungskontakt über das Identitätsregister erfolgen.
- Es werden per Definition verschiedene Bereiche (auch Sektoren bzw. Tätigkeitsbereiche genannt) gebildet. Bei bereichsübergreifender Kommunikation wird jeweils das bPK des anderen Bereichs beim Identitätsregister abgefragt (sofern keine Rechtsgrundlage für

den Datenaustausch besteht wird auch kein bPK übermittelt). Es wird vorgeschlagen, dass die Anzahl der Bereiche bei ca. 10 bis 20 liegen sollte (S.9 im bPK-Modell).

- Für die Kommunikation mit dem OZG-Nutzerkonto und dem angestrebten DC könnten zwei bereichsübergreifende bPK gebildet werden.
- Für definierte Kernregister der Verwaltung könnten die jeweiligen bPK flächendeckend ausgerollt werden. Für die Festlegung dieser Kernregister könnten z.B. die Vergleichsregister von DESTATIS oder genannte Register aus dem NKR-Gutachten herangezogen werden.

Aus der folgenden Grafik 6 wird der Kommunikationsfluss im bPK-Modell besser ersichtlich, alle Bereiche verfügen hier über einen eigenen verschlüsselten Identifikator. In der Mitte befindet sich das ID-Register mit den Personenbasisdaten der Bürgerinnen und Bürger. Dort findet auch die Berechnung der Stammzahlen und der bPK für alle Verwaltungsbereiche statt:



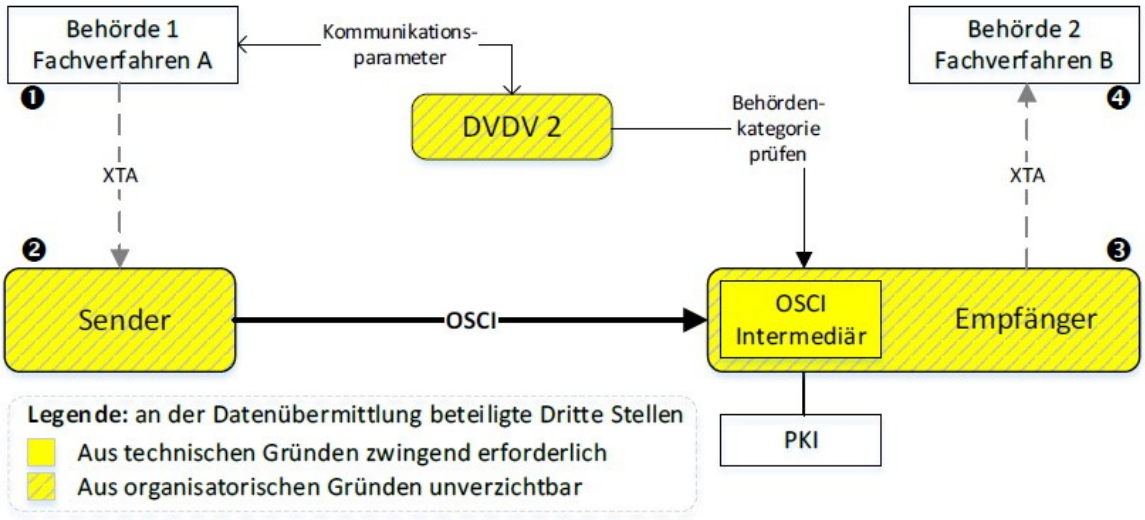
Grafik 6: Datenfluss im Rahmen der bPK Berechnung und Verteilung

6.3 Einheitlicher Identifier auf Basis eines erweiterten 4-Corner-Modells mit mehreren Bereichen

Mit der Erkenntnis, dass schon heute eine Vielzahl von Datenaustauschbeziehungen in der öffentlichen Verwaltung besteht und eine Lösung für das registerübergreifende Identitätsmanagement möglichst auf vorhandenen Strukturen aufbauen und zugleich die heutige dezentrale Registerstruktur erhalten bleiben sollte, wurde seitens der Koordinierungsstelle für IT-Standards (KoSIT) ein Modell für die gemeinsame Expertengruppensitzung am 14./15. Januar 2020 ausgearbeitet (Anlage) und vorgestellt, das zwar wie das Basismodell mit einem Identifier - der Steuer-ID - operiert, jedoch zusätzliche Sicherungsmaßnahmen gegen eine unrechtmäßige Zusammenführung von Daten zu einem umfassenden Persönlichkeitsprofil beinhaltet.

Weitere Merkmale des vorgestellten Modells sind:

- Übernahme der bPK-Vorstellung, dass es verschiedene Bereiche und damit bereichsübergreifende Datenübermittlungen gibt, die die Steuer-ID enthalten.
- Die Datenübermittlung zwischen zwei Behörden aus unterschiedlichen Bereichen – sofern hier eine Rechtsgrundlage besteht - erfolgt nicht direkt, sondern über „Dritte Stellen“, gemeint sind damit die Transporteure und der zentrale Verzeichnisdienst.
- Diese Dritten Stellen müssen öffentliche Stellen im Sinne des § 2 BDSG sein. Sie kontrollieren und protokollieren den bereichsübergreifenden Datenaustausch.
- Es wird eine Ende-zu-Ende-Verschlüsselung vorgesehen, die Dritten Stellen können ihre Aufgaben ohne Kenntnis des Nachrichteninhalts („doppelte Umschläge“ – ähnlich einer Briefwahl) erbringen, sie kennen lediglich die Metadaten der Datenübermittlung, insbesondere prüfen sie die Identität der Kommunikationspartner.
- Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle als Vermittlungsdienst oder Verzeichnisdienst unter Angabe der Kommunikationspartner und dem Zweck vermittelt werden. Diese versorgt die Transporteure mit den für den Transport erforderlichen Angaben. Eine Vermittlung ist nur dann möglich, wenn zuvor für den angegebenen Zweck und die angegebenen Kommunikationspartner ein Eintrag im Vermittlungs- bzw. Verzeichnisdienst besteht. Datenübermittlungen, für die keine Rechtsgrundlage besteht oder bei denen die Angaben zu Sender, Empfänger und Zweck nicht zueinander passen, können wegen fehlendem Eintrag eines Dienstes nicht vermittelt werden.
- Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten, transparenten Prozess erfolgen.
- Verwendung offener Standards: alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt.



Grafik 7: 4-Corner-Modell –Infrastruktur in der Innenverwaltung (schematisch)

Das in Grafik 7 dargestellte 4-Corner-Modell mit einem zentralen Deutschen Verwaltungsdiensteverzeichnis (DVDV) beim ITZBund wird in Grundzügen bereits heute für die Innenverwaltung eingesetzt.

6.4 Gespräche in den Expertengruppen

In der gemeinsamen Sitzung der Expertengruppe 1 „Registerarchitektur“ und 2 „Identifier“ am 14./15. Januar 2020 wurden die unter 6.2 und 6.3 dargestellten Modelle – mit Blick darauf, dass sie beide Instrumente zum Schutz des Rechts auf informationelle Selbstbestimmung aufweisen – näher untersucht und intensiv, wenn auch nicht abschließend erörtert.

Es wurde auf fachlicher Ebene Konsens darüber erzielt, dass die beiden letzten Modelle grundsätzlich die an sie gestellten Aufgaben, insbesondere die korrekte Zuordnung von Personendatensätzen, erfüllen. Beide Modelle berücksichtigen zudem verfassungs- und datenschutzrechtliche Anforderungen, wobei nach der nicht unbestritten gebliebenen Auffassung der teilnehmenden Vertreter der Datenschutzkonferenz das bPK-Modell mit mehreren Identifikatoren ein höheres Schutzniveau und ein geringeres verfassungsrechtliches Risiko gegenüber einem einheitlichen Identifier auf Basis des erweiterten 4-Corner-Modells aufweise, da die Steuer-ID vom BFH mit dem Hinweis auf ihre bereichsspezifisch begrenzte Verwendung gerechtfertigt wurde. Die Möglichkeit der angestrebten OZG-Umsetzung ist ebenfalls bei beiden Modellen gegeben. Auch die Vorteile einer hohen Datensparsamkeit bei der Verwen-

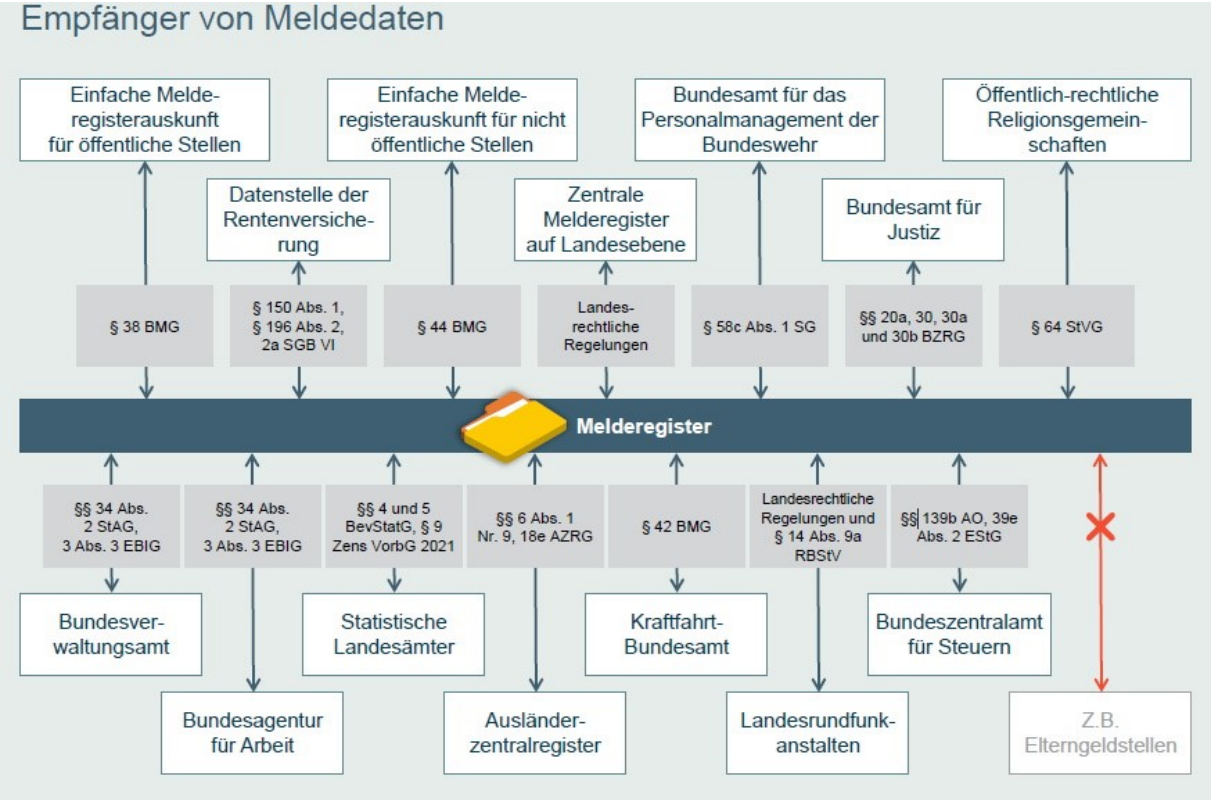
dung eines Identifiers gegenüber dem heutigen Abgleich von Personenbasisdaten für Datenübermittlungen wurden bei beiden Modellen anerkannt. Auch bestand Konsens bei den Teilnehmern der Sitzung, dass weder der gegenwärtige Zustand noch eines der Modelle bei einem politischen Systemwechsel unter Aufgabe der Rechtsstaatlichkeit einen Schutz gegen eine Zusammenführung von Daten gewährleisten.

Es wurden in der Sitzung zudem die Unterschiede beider Modelle erörtert und Argumente insbesondere zu Nutzen, Kosten und Risiken ausgetauscht. In der Folge wurde seitens BMI ein Auftrag vergeben, in dem Aufwände und Kosten kurzfristig in einem ersten Schritt zumindest grob geschätzt werden sollten. Nähere Ausführungen zu den Ergebnissen der Schätzung finden sich unter Punkt 6.6 dieses Berichts.

Im Ergebnis der gemeinsamen Sitzung der beiden Expertengruppen wurde kein Konsens erzielt in der Bewertung der Modelle im Hinblick auf Verfassungs- und Datenschutzkonformität.

Tatsächlich bietet das erarbeitete konzeptionelle bPK-Modell ein in sich stimmiges, wenn auch sehr komplexes Gesamtkonzept für die Datenaustauschbeziehungen der deutschen Registerlandschaft. Es dürfte den verfassungs-und datenschutzrechtlichen Anforderungen sehr gut gerecht werden, gleichwohl trifft das Modell auf eine zwischen Bund, Ländern und Kommunen aufgebaute, gewachsene IT-Infrastruktur mit erfolgreich bestehenden Datenaustauschbeziehungen zwischen verschiedenen Bereichen (im Sinne des bPK-Modells). So müsste der in der Praxis bestehende Datenaustausch in allen Fachbereichen neu organisiert werden, was dem Ziel, die Registermodernisierung in Deutschland zu beschleunigen, deutlich entgegensteht. Anstatt die Verwaltung in die Lage zu versetzen, schnellstmöglich Personendatensätze korrekt zuordnen zu können, müsste zunächst eine Reorganisation bestehender Datenaustauschprozesse stattfinden, die heute auf gesetzlicher Grundlage und nicht zu beanstandenden IT-Sicherheitsstandards durchgeführt werden. Als Beispiel hierfür dient der jahrelang erfolgreich bestehende Datenaustausch zwischen den Meldebehörden und den Rentenversicherungsträgern nach § 6 der 2. BMeldDÜV. Die Komplexität verdeutlicht folgende Grafik 8 aus dem Bericht des Normenkontrollrats[4]. Es wird deutlich, dass eine Vielzahl öffentlicher Stellen Meldedaten für ihre Aufgabenerfüllung benötigen.

[4] Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren. Oktober 2017 Auftraggeber Nationaler Normenkontrollrat S. 22



Grafik 8: Aus Gutachten für Normenkontrollrat: „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren“ S. 22 unten.

Auch wenn in der fachlichen Diskussion eine Definition der bPK-Bereiche (bzw. Sektoren) nicht abgeschlossen und mit der Arbeitshypothese gearbeitet wurde, dass ein Bereich in etwa einem Ressort der Bundesregierung entsprechen könnte, ist ersichtlich, dass heute bereits in sehr hohem Maße bereichsübergreifender Datenaustausch stattfindet, z.B. zwischen der Innenverwaltung und der Justiz (Bundeszentralregister), Arbeit (Bundesagentur für Arbeit-Datenbanken), Soziales (Datenstelle der Deutschen Rentenversicherung), Verteidigung (Bundeswehr) etc. Eine Reduktion auf wenige Sektoren könnte die Komplexität verringern, erfordert aber gleichwohl den Aufbau des Systems in mehreren Schritten.

Eine Anwendung gemäß bPK-Modells dürfte in folgenden Schritten erfolgen:

1. Aufbau eines neuen eigenständigen Identitätsregisters, das unabhängig von der heutigen ID-Nummer-Datenbank des BZSt eingerichtet werden müsste, da die Finanzverwaltung mit ihren eigenen Finanz-bPK auf das (neutrale) Identitätsregister zugehen sollte, um Interessenkonflikte zu vermeiden. Der Aufbau eines eigenständigen Identitätsregisters entspricht nicht den vom Bundeskabinett beschlossenen Eckpunkten.
2. Anbindung von bspw. ca. 5.000 kommunalen Meldebehörden sowie Standesämter und weiterer kommunaler Fachverfahren und Register, da diese aufgrund ihrer be-

reichsübergreifenden Kommunikation, z.B. mit Gesundheits- Justiz- und Finanzbehörden, direkt an das Identitätsregister angebunden werden müssten. Alternativ wäre die Einführung von zentralen Kernregistern, ähnlich wie in Österreich mit zentralem Melderegister, zentralem Personenstandsregister, Unternehmensregister, jeweiligen Ergänzungsregistern etc. erforderlich, entspräche jedoch nicht den vom Bundeskabinett beschlossenen Eckpunkten.

3. Nach Einrichtung einer Stammzahlenbehörde – hier stellt sich die Frage, ob Identitätsregister- und Stammzahlenbehörde in der gleichen Einrichtung verortet werden dürften – erfolgt der Roll-out der bPK in alle Bereiche. Der Roll-out der bPK müsste alle kommunalen Register umfassen, da ein Großteil der elektronischen Verwaltungskommunikation zwischen kommunalen Einrichtungen stattfinden dürfte. Die heutigen IT-Kommunikationsstrukturen über die jeweiligen Melderegister könnten hierfür nicht genutzt werden.
4. Bestehende Kommunikationsstrukturen und IT-Infrastrukturen müssten parallel angepasst werden, weil die gleichzeitige neue Anbindung der Behörden an das Identitätsregister und der gleichzeitige Roll-out der bPK in alle dezentralen Register nicht denkbar ist.

Abschließend wird im Ergebnis die Datenkommunikation, die heute bereits auf rechtlicher Grundlage besteht, in gleichem Umfang wiederhergestellt. Dabei ergäben sich u.a. folgende Nebenwirkungen:

1. alle Fachverfahren in diesen Bereichen sind umzugestalten, da statt der (bereits heute häufig schon) gespeicherten Steuer-ID nun – je nach bPK-Lösungsvariante - mehrere bPK nebeneinander zu speichern wären, um den heutigen Datenaustausch mit dem gleichen Zweck zu ermöglichen,
2. Verwaltungsverfahren, die bereits abgeschlossen sind, dürften wohl nicht nachträglich mit einer bPK auszustatten sein, aber bereits begonnene Verwaltungsverfahren müssten bei der Umstellung migriert werden auf bPK,
3. (insbesondere kommunale) Behörden, die mehrere Tätigkeitsbereiche umfassen, müssten dann selbst mehrere bPK für ihre einzelnen Bereiche verwenden.

Ziel beider Modelle muss sein, einerseits den Datenaustausch, für den es eine zugehörige Rechtsgrundlage gibt, effizient zu ermöglichen und gleichzeitig sicherzustellen, dass ein elektronischer Datenaustausch, für den es keine rechtliche Grundlage gibt, unterbunden wird. Die beschriebene teil- oder vollumfängliche Profilbildung darf nicht möglich sein. Während im bPK-Modell diese Eigenschaft seitens der Datenschutzbeauftragten als inhärent zugeschrieben wird, soll ein Blick auf die datenschutzrechtlichen Sicherungsmechanismen in

der Variante mit einheitlichem Identifier auf Basis des erweiterten 4-Corner-Modells gerichtet werden:

- die Einrichtung mehrerer Bereiche,
- die Kontrolle bereichsübergreifender Datenaustausche über die Verwendung Dritter Stellen,
- die Einrichtung von Diensten in einem unabhängigen Vermittlungs- bzw. Verzeichnisdienst auf Grundlage rechtlicher Regelungen, da ansonsten ein Datenaustausch unmöglich ist,
- die Verwendung transparenter Interoperabilitätsstandards auch für die Aufsichtsbehörden zur Wahrnehmung ihrer Kontrollaufgaben.

Bei Betrachtung der Gefahr durch einen potentiellen Außentäter wird deutlich, dass die heute bereits eingesetzte PKI-Verschlüsselungsinfrastruktur vor einem Belauschen der Kommunikation auf den Transportwegen schützt. Mithilfe des Prinzips des doppelten Umschlags mit getrennten Transport- und fachlichen Inhaltsdaten könnte ein Angreifer möglicherweise die Datenwege einer Nachricht in Erfahrung bringen (also welche Organisationseinheiten der Behörden untereinander kommunizieren), jedoch nicht den Inhalt. Ein Angriff auf das DVDV wäre nicht lohnenswert, da hier nicht Daten einzelner Personen gespeichert werden, sondern das DVDV als eine Art Adressbuch („gelbe Seiten“) für öffentliche Stellen agiert mit einer Übersicht aller (auf gesetzlicher Grundlage) eingerichteter Dienste für die Behördenkommunikation. Auch hier stellt nicht der Identifier, die Steuer-ID, eine Gefahr dar, da ein Angreifer ebenso gut mit Namensbestandteilen operieren könnte und nicht auf die Kenntnis der jeweiligen Steuer-ID angewiesen ist. Der Nutzen der Steuer-ID, die eindeutige Zuordnung von Personenbasisdaten einer Person in verschiedenen Registern der öffentlichen Verwaltung zu gewährleisten, dürfte für den Angreifer kaum entscheidend sein.

Bei Betrachtung der Gefahr durch einen potentiellen Innentäter ist in der Variante miteinheitlichem Identifier auf Basis des erweiterten 4-Corner-Modells eine elektronische Abfrage von Fachdaten einer Person, für die es keine Rechtsgrundlage gibt, unmöglich, weil im DVDV auch kein Dienst besteht. Um hier Daten abzurufen, müsste sich ein Innentäter als Behörde ausgeben, mit deren Fachverfahren und Verschlüsselungssystemen arbeiten und einen elektronischen Datenabruf durchführen (der protokolliert würde), für den es eine rechtliche Grundlage gibt. Hierüber lassen sich auch bei Kenntnis eines bestimmten Identifiers, der Steuer-ID, keine Daten, für die keine rechtliche Datenübermittlung vorgesehen ist, zusammenführen. Möglich wäre der Missbrauch der dem Innentäter eingeräumten dienstlichen Befugnisse zu dienstlich nicht erlaubten Abfragen. In diesem Fall bietet auch das bPK-Modell

keinen weitergehenden Schutz. Derartige Fälle werden üblicherweise durch disziplinarrechtliche Konsequenzen, Straf- und Bußgeldvorschriften sowie Protokollierung und Kontrollmechanismen abgesichert.

Die Kontrollelemente der Variante mit einheitlichem Identifier auf Basis des erweiterten 4-Corner-Modells liegen neben einer abgesicherten IT-Infrastruktur insbesondere in den beteiligten Dritten Stellen (Transport und Vermittlungsdienst) für bereichsübergreifende Datenübermittlungen, die staatlicher Kontrolle unterliegen müssen und die lediglich die Metadaten der Datenübermittlung (keine Kenntnis des Nachrichteninhalts) benötigen dürfen, um ihre Aufgaben erbringen zu können. Dies sind bewusst abstrakt gehaltene - jedoch zumindest in eine Verordnung aufzunehmende - Anforderungen an die Infrastruktur, um die Teilnahme der heute diversen Registerstrukturen an der Verwendung des Identifiers, der Steuer-ID, zu ermöglichen. In der Innenverwaltung hat sich diese Infrastruktur seit Jahren bewährt. Sie wird analog in der Justizverwaltung mit der Kommunikationsstruktur SAFE verwendet.

Die Einführungsphase dürfte sich mit diesem Modell deutlich einfacher gestalten lassen als mit dem bPK-Modell. So wird die Steuer-ID als möglichem registerübergreifenden Identifier bereits heute in zahlreichen Registern gespeichert. Zudem verfügen insbesondere die Landes- und Kommunalebenen - insbesondere mit den Meldebehörden als Dreh- und Angelpunkte - über eine etablierte Struktur, die für den Roll-Out der Steuer-ID genutzt werden kann. So können im Ergebnis die Register nach einer festzulegenden Reihenfolge flexibel ausgerollt werden, indem die Steuer-ID in diesen Registern jeweils zugespeichert wird. Mit der Zuspeicherung der Steuer-ID im dezentralen Fachregister können auch - abhängig vom jeweiligen Fachregister und dortigen fachlichen Anforderungen - Namen und Adressdaten etc. dezentral erhalten bleiben. Es können für jedes Register die Anforderungen individuell behandelt werden. Werden die eigenen Datenbestände häufig verwendet (liegt also kein „Entscheidungsregister“ vor) und sind die wichtigsten Kommunikationspartner einer Registerstelle bereits mit der Steuer-ID ausgestattet, dürfte sich entsprechend ein zeitlich früher Roll-out anbieten.

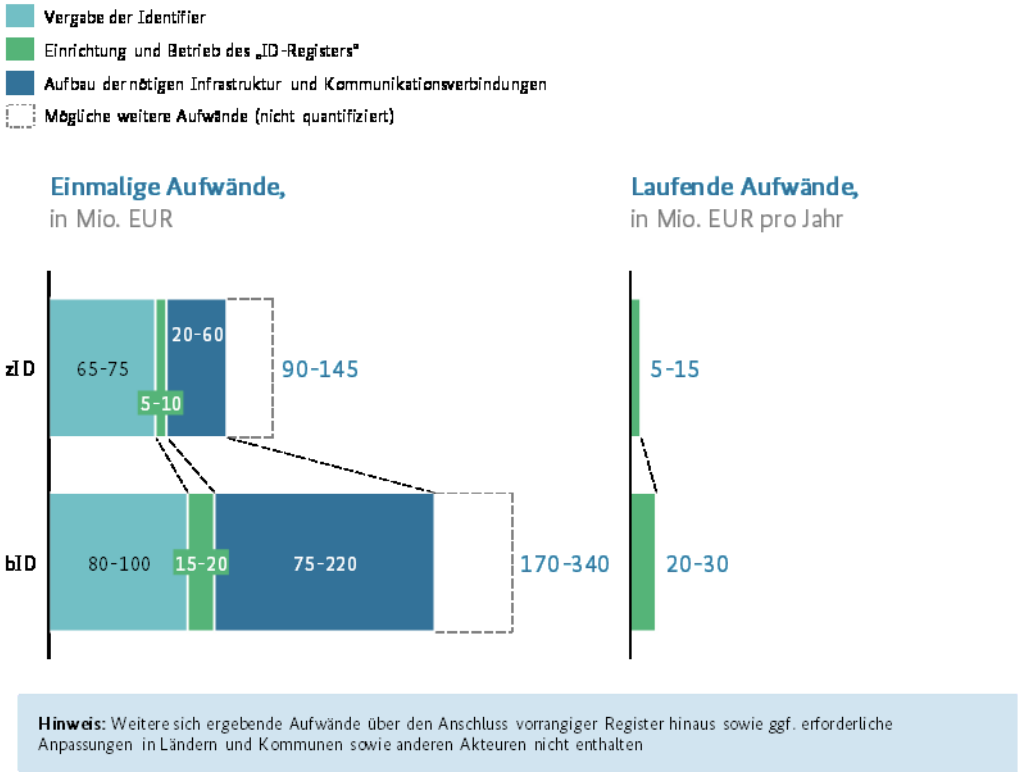
6.5 Grobe Schätzung der Aufwände, Kosten und Realisierungszeiträume

In der Bewertung der beiden Modelle – der Variante mit einheitlichem Identifier auf Basis des erweiterten 4-Corner-Modells und der Variante des bPK-Modells – in der gemeinsamen Expertengruppensitzung wurde deutlich, dass neben Nutzen und Risiken auch ein Vergleich im Hinblick auf Aufwände und Realisierungszeiträume angefertigt werden solle. In der Folge wurde McKinsey & Company mit einer möglichst präzisen Aufwandsschätzung der beiden

vorgeschlagenen Modelle beauftragt, die seitens McKinsey als Modell mit zentralem Identifier (zID) und mit bereichsspezifischer Identifier (bID) bezeichnet wurden. Hierfür wurden die Modelle weitergehend konkretisiert, um eine Vergleichbarkeit zu ermöglichen.

Die in den „Kernbotschaften der Aufwandsschätzung“ enthaltenen Ergebnisse (Anhang 3) gehen für die Einrichtung und den Betrieb des zID-Modells mit einmaligen Kosten von 90 bis 145 Mio. EUR, laufenden Kosten von 5 bis 15 Mio. EUR sowie einer Umsetzungsdauer von drei bis sechs Jahren aus. Für die Einrichtung und den Betrieb des bID-Modells sei mit einmaligen Kosten von 170 bis 340 Mio. EUR, laufenden Kosten von 20 bis 30 Mio. EUR sowie einer Umsetzungsdauer von sieben bis zehn Jahren zu rechnen.

Abbildung 5
Aufstellung der einmaligen und laufenden finanziellen Aufwände je Modell.



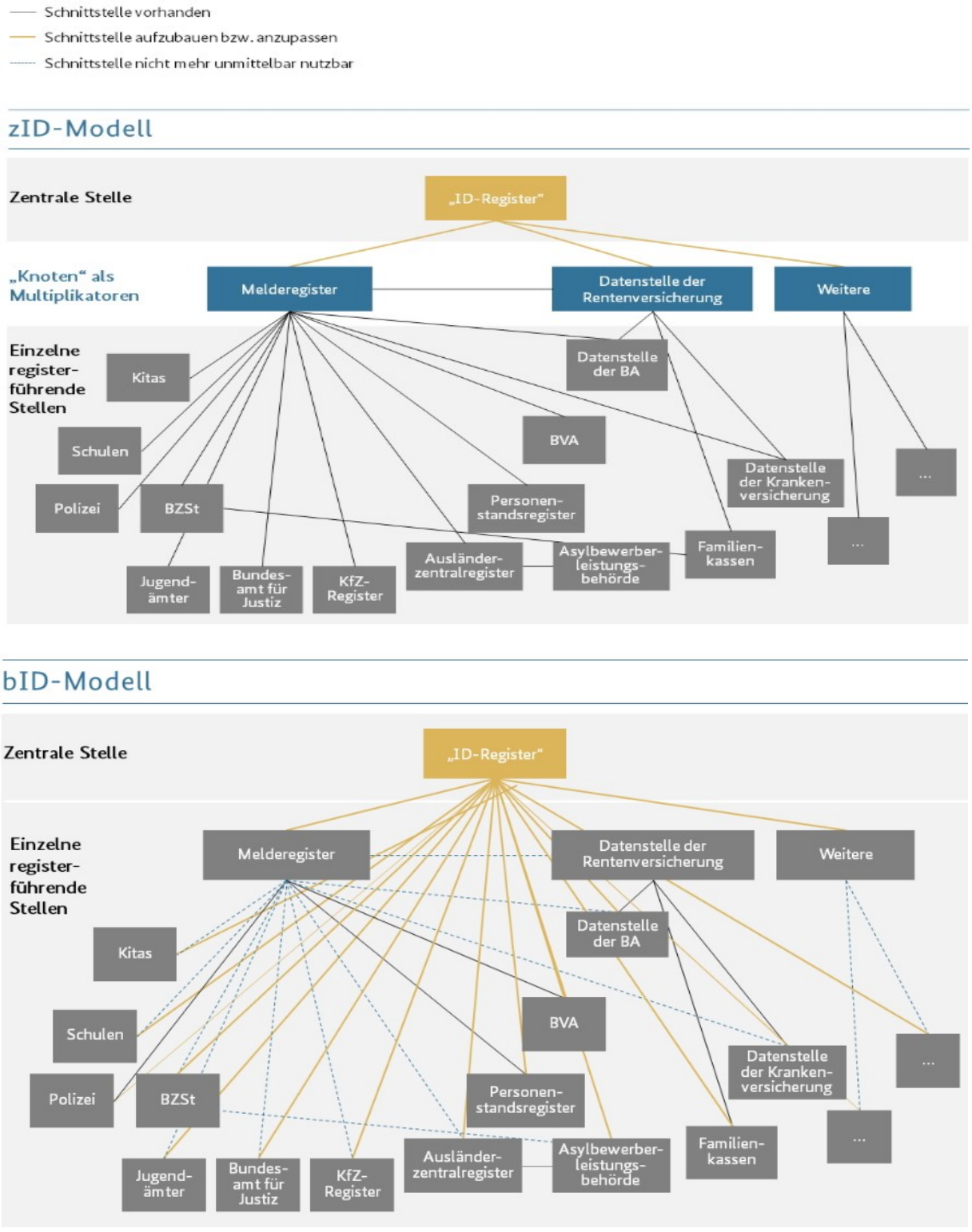
Grafik 9: Aus „Aufwandsschätzung für die Einführung eines registerübergreifenden ID-Managements“, S. 28.

Dabei beziehen sich diese ermittelten Aufwände auf die Inbetriebnahme eines registerübergreifenden Identitätsmanagements und Anschluss von 26 von McKinsey als vorrangig identifizierten Registern, z.B. das AZR, Melde- und Personenstandsregister, Pass- und Personalausweisregister etc. Nicht betrachtet wurden aufgrund der Komplexität die weiteren Register und Fachverfahren auf kommunaler Ebene, z.B. Schul- und Gesundheitsbehörden, Polizeien, Jugendämter oder weitere örtliche Träger.

Abbildung 6

Nachträglich angepasst am 10.03.2020

Schematischer Vergleich der sich ergebenden Netztopologien zwischen zID- und bID-Modell. Kernunterschied ist die Möglichkeit des zID-Modells, lokale „Knoten" für die Verteilung des Identifiers und den Datenaustausch zu betreiben, während im bID-Modell ein direkter Kontakt aller Akteure zum „ID-Register" erforderlich scheint.



Grafik 10: Aus „Aufwandsschätzung für die Einführung eines registerübergreifenden ID-Managements", S. 38.

Auch der im bPK-Modell erforderliche Anschluss dezentraler privatwirtschaftlicher Akteure, wie etwa aller Arbeitgeber, Banken und Versicherungen, die heute bereits mit der Steuer-ID operieren und mit bPK versorgt werden müssten, wurde nicht betrachtet.

Jedoch wird in der Aufwandsschätzung darauf hingewiesen, dass „im Fall des bID-Modells … zu erwarten [wäre], dass diese vorangehend genannten Aufwände höher ausfallen als bei der Umsetzung des zID-Modells, da hier eine komplexere Netztopologie vorliegt, die Funktion bestehender „Knoten“ wie etwa der Meldebehörden nur noch eingeschränkt nutzbar wäre und zudem davon ausgegangen wird, dass in allen Systemen, die bisher die Steuer-ID nutzen (z.B. bei Banken, Versicherungen und Arbeitgebern), diese durch die Finanz-bID ersetzt werden müsste“. Die nötige umfangreiche Anpassung der Fachverfahren stelle „einen signifikanten quantifizierten Aufwandstreiber im bID-Modell dar.“

Die deutlich längere Realisierungszeit für das bID-Modell von ca. 4 Jahren steht den Zielen der raschen Registermodernisierung und der Umsetzung des Registerzensus entgegen. Auch die vom Normenkontrollrat im Gutachten „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren“ beschriebenen Einsparpotentiale lassen sich in dieser Zeit nicht heben und sind grundsätzlich als Opportunitätskosten dem bID-Modell zuzurechnen.

6.6 Roll-out der Steuer-ID als registerübergreifendem Identifier in die öffentliche Verwaltung

Ein konkreter Roll-out-Plan, um die Steuer-ID in den dezentralen Fachregistern zuzuspeichern, muss separat festgelegt werden. Zunächst wird ein sukzessives Vorgehen mit vier Gruppen vorgeschlagen:

1. zuerst könnten die bereits heute (über die Meldebehörden) an die ID-Nummer-Datenbank des BZSt zuliefernden Register der Innenverwaltung die Steuer-ID zuspeichern, also insbesondere die Personenstandsregister und das AZR. Dabei könnten diese entweder eine direkte Verbindung, z.B. für das MAV, zum Identitätsregister herstellen oder die bestehenden Kommunikationswege nutzen und über die Melderegister mit der Steuer-ID versorgt werden,

2. anschließend sollten alle Register, die eine bedeutsame Rolle für den ab 2024 nach europäischen Vorgaben jährlich durchzuführenden Registerzensus spielen, ausgerollt werden, auch um die im NKR-Bericht dargestellten hohen Einsparpotentiale zu heben,

3. alle Register, die aufgrund ihrer zugehörigen Verwaltungsleistungen sehr stark von aktuellen Personenbasisdaten abhängig sind,

4. anschließend sog. „Entscheidungsregister“, bei denen zunächst aktuelle Personenbasisdaten für eine bestimmte Verwaltungstätigkeit benötigt werden, danach jedoch die Datensätze tendenziell selten angefasst werden.

Sicherlich wird ein Roll-out-Plan ausreichend Flexibilität aufweisen müssen, um laufende Gesetzgebungsvorhaben zeitnah unterstützen zu können. In Frage kommen hier zum gegenwärtigen Zeitpunkt bspw. neben dem Registerzensusvorbereitungsgesetz die Vorhaben zum Digitale-Familienleistungen-Gesetz im Rahmen des Vorhabens „ELFE“ (Elektronische Leistungen für Eltern) oder zur Grundrente oder der Altersvorsorgepflicht für Selbstständige und Freiberufler.

7. Rechtliche Ausgestaltung und Gesetzentwurf

Die erforderlichen rechtlichen Regelungen werden, vorbehaltlich der weiteren Abstimmungen im Gesetzgebungsverfahren innerhalb der Bundesregierung, mit einem Entwurf eines Registermodernisierungsgesetzes in Form eines Artikelgesetzes erstellt. In einem neuen Stammgesetz (Arbeitstitel: „Gesetz zur Einführung eines Basisdatenregisters (Basisdatenregistergesetz)“) werden Regelungen zur Errichtung und Betrieb des Basisdatenregisters, zum darin enthaltenen Datenkranz, zur Datenübermittlung zwischen Basisdatenregister und Fachregistern sowie die erforderlichen datenschutzrechtlichen Sicherungen geregelt. In den sich daran anschließenden Änderungsgesetzen der einzelnen Fachgesetze wird der dortige fachliche Änderungsbedarf geregelt.

8. Bewertung, offene Fragen und Ausblick

Aus der fachlichen Arbeit ergibt sich für die BLAG Registerübergreifendes Identitätsmanagement und BMI, dass die Steuer-ID als zukünftiger Identifier und die Steuer-ID-Nummer-Datenbank des BZSt als Ausgangspunkte für ein deutlich verbessertes Identitätsmanagement in der Innenverwaltung - und implizit darüber hinaus für weitere Register, die sich stark auf personenbezogene Daten stützen, grundsätzlich geeignet sind.

In der Diskussion zu verfassungs- und datenschutzrechtlichen Fragestellungen innerhalb der beratenden Expertengruppen wurde seitens der Datenschutzbeauftragen vorgetragen, dass neben der Vorgabe einer vorzugsweisen dezentralen Haltung von Fachdaten und dem üblichen Instrumentarium zur Sicherung der Rechtmäßigkeit von Datenübermittlungen (wie erforderliche Rechtsgrundlagen, Zweckbindung, Protokollierung, Kontrollmaßnahmen, Sanktionierung) zusätzliche Sicherungsmaßnahmen eingerichtet werden sollten, um das Risiko einer unrechtmäßigen Zusammenführung von Fachdaten zu einer Person, das bei der Nutzung eines einzigen Identifiers per se erhöht sei, auszuschließen. Für die Einrichtung dieser Sicherungsmaßnahmen kann das Basismodell derart konzeptionell verändert werden, dass

eine Umsetzung mit einem Identifier, der Steuer-ID, ermöglicht wird. Die verfassungsrechtliche Notwendigkeit zusätzlicher Sicherungsmaßnahmen und deren Ausprägung blieb ohne Konsens.

Einer der wesentlichen Ausgangspunkte des registerübergreifenden Identitätsmanagements ist es, möglichst die Vorteile etablierter Strukturen zu nutzen. So stehen bereits wie ausgeführt mit der Steuer-ID, der ID-Nummer-Datenbank mit ca. 105 Mio. Personenbasisdaten, einer mit Public-Key-Infrastruktur und zentralem Verzeichnisdienst ausgestatteten IT-Kommunikationsinfrastruktur (z.B. in der Innenverwaltung) eine Reihe wichtiger Bausteine für ein funktionierendes registerübergreifendes Identitätsmanagement zur Verfügung. Sie ermöglichen eine Realisierung des registerübergreifenden Identitätsmanagements mithilfe der Steuer-ID, ohne die heute bestehenden Datenaustauschbeziehungen zurückbauen zu müssen. Damit kann ein bedeutsamer Beitrag zur Beschleunigung der Digitalisierung der öffentlichen Verwaltung geleistet werden. Die korrekte Zuordnung von Personenbasisdaten ist Grundlage einer modernen digitalen Registerlandschaft der öffentlichen Verwaltung. Dies gilt umso mehr, wenn die Datenhaltung auch zukünftig in einer Vielzahl föderaler dezentraler Register organisiert, und nicht wie z.B. in Österreich zunächst zentrale Register für Personen, Firmen, Vereine und zentrale Ergänzungsregister etc. eingerichtet werden sollen.

Darum sprechen sich im Ergebnis die BLAG Registerübergreifendes Identitätsmanagement und das BMI für eine Umsetzung mithilfe der Steuer-ID aus dem Finanzbereich aus. Für gegebenenfalls erforderliche zusätzliche Sicherungen gegen unzulässige Datenzusammenführungen könnte auf das dargestellte 4-Corner-Modell zurückgegriffen werden, das in Grundzügen bereits heute erfolgreich in der Innenverwaltung eingesetzt wird.

Im Hinblick auf den Betrieb und die fachliche und technische Weiterentwicklung des Identitätsregisters bzw. der ID-Nummer-Datenbank werden zwischen BMI und BMF gegenwärtig offene Fragen der Governance besprochen. Hier geht es insbesondere um die Aspekte zuständige Registerbehörde, Fachaufsicht, Erweiterung der Kapazitäten für die Qualitätssicherung und den Roll-out der Steuer-ID in die als priorisiert angesehenen Register. Da wie ausgeführt die Sicht der Finanzverwaltung und die Sicht der identitätsregisternutzenden Stellen auf die gleiche Datenbank unterschiedlich sein werden - auch wenn die Schnittmenge der von beiden Registern genutzten Datenfelder sehr groß ist (vgl. Grafik 3) - sollte eine enge fachliche und technische Abstimmung der Ressorts stattfinden.

Die im Zwischenbericht behandelte Alternative zur Nutzung der ID-Nummer Datenbank im Bereich der Finanzverwaltung, also der Aufbau eines eigenen Identitätsregisters für das registerübergreifende Identitätsmanagement soll zunächst nicht weiterverfolgt werden.

Stand heute wird für die gesetzliche Umsetzung ein Kabinettbeschluss zum Ende des 2. Quartals 2020 angestrebt, um ein Inkrafttreten für das 1. Quartal 2021 zu ermöglichen.

Im Anschluss an das Inkrafttreten des Gesetzes soll für die nächste Frühjahrssitzung der IMK über die Fortschritte der fachlichen Arbeit und den angestrebten Beginn der Realisierungsphase erneut zum Sachstand berichtet werden.

Abbildungsverzeichnis

Abkürzungsverzeichnis

AO	Abgabenordnung
AZR	Ausländerzentralregister
BFH	Bundesfinanzhof
BMF	Bundesministerium der Finanzen
BMAS	Bundesministerium für Arbeit und Soziales
BMI	Bundesministerium des Innern, für Bau und Heimat
bPK	bereichsspezifische Personenkennziffer
BVerfG	Bundesverfassungsgericht
BvF	Registerzeichen beim Bundesverfassungsgericht für Normenkontrollverfahren nach Art. 93 Abs. 1 Nr. 2 GG
BZSt	Bundeszentralamt für Steuern
DSGVO	Datenschutzgrundverordnung
DC	Datencockpit
DSK	Datenschutzkommission
DVDV	Deutsches Verwaltungsdiensteverzeichnis
ELFE	Elektronische Leistungen für Eltern
ID-Nr.-Datenbank	Steueridentifikationsnummerdatenbank
ID-Register	Identitätsregister
IMK	Innenministerkonferenz
ITZBund	Informationstechnikzentrum des Bundes
KiStAM	Kirchensteuerabzugsmerkmal
KoSIT	Koordinierungsstelle für IT-Standards
MAV	Maschinelles Abfrageverfahren
MB	Meldebehörde(n)
MPK	Ministerpräsidentenkonferenz, Gremium der Bundesländer
NKR	Normenkontrollrat

OSCI	Online Services Computer Interface, Reihe verschiedener Protokollstandards für den Austausch fachlicher Inhaltsdaten auf XML-Basis zwischen Behörden
OZG	Onlinezugangsgesetz bzw. Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen
PKI	Public-Key-Infrastruktur, Systemtyp in der Kryptologie
PStV	Personenstandsverordnung
RBM	Rentenbezugsmitteilung(en)
SAFE	Secure Access to Federated e-Justice / e-Government Sichere elektronische Identitäten in einem föderalen Umfeld.
Steuer-ID	Steueridentifikationsnummer
2. BMeldDÜV	Zweite Bundesmeldedatenübermittlungsverordnung

Anhang 1: Digitalkabinett Eckpunkte vom 18. November 2019

Eckpunkte

zum registerübergreifenden Identitätsmanagement

als Teil der Registermodernisierung

Wird die Verwaltung zunehmend digitalisiert, muss auch in der digitalen Kommunikation gewährleistet sein, dass Personenverwechslungen ausgeschlossen und die betroffenen Bürgerinnen und Bürger eindeutig identifiziert werden. Das registerübergreifende Identitätsmanagement bietet zudem die Chance, den Zensus ohne aufwändige und kostenträchtige Befragung natürlicher Personen registerbasiert durchzuführen und entlastet damit die Bürgerinnen und Bürger und baut Bürokratie ab. Ohne eine Modernisierung der Registerlandschaft kann „once only“ nicht umgesetzt werden: Wir wollen Bürgerinnen und Bürgern die Möglichkeit geben, bei der Verwaltung bereits vorhandene Daten nicht immer wieder eingeben zu müssen, wenn sie Leistungen der Verwaltung in Anspruch nehmen wollen. Dies geht nicht ohne verbesserten Datenaustausch, bei dem gewährleistet sein muss, dass Personenverwechslungen ausgeschlossen sind. Gleichzeitig muss die Ausgestaltung selbstverständlich verfassungs- und datenschutzkonform erfolgen. Hierzu sollen die in der Datenschutz-Grundverordnung enthaltenen Chancen zu Gunsten des Datenschutzes genutzt werden: Privacy by Design, Datensparsamkeit und bessere Datenqualität. Wir werden dabei Vorkehrungen treffen, die verfassungsrechtlich unzulässige Datenverknüpfungen ausschließen.

Die Registermodernisierung bietet die Chance, die Transparenz für Bürgerinnen und Bürger zu erhöhen und sichtbar zu machen, welche Stelle welcher anderen Stelle wann und zu welchem Zweck ihre Daten übermittelt hat. Diese Funktion kann von einem zukünftigen Datencockpit wahrgenommen werden.

Bei dem registerübergreifenden Identitätsmanagement handelt es sich um ein Vorhaben, das das Arbeiten der Verwaltungen in Deutschland verändern wird. Es wird erhebliche Investitionen notwendig machen und muss die notwendige Akzeptanz in der Bevölkerung erreichen. Nur dann können die Chancen, die das Projekt bietet, zu einem dauerhaften Erfolg führen und den Bürgerinnen und Bürgern nutzen.

Auf Grundlage der bereits erfolgten Vorarbeiten zeichnen sich folgende Kernelemente ab:

1. Zur eindeutigen Zuordnung in den Datenbeständen der öffentlichen Verwaltung werden für natürliche Personen, die ein Verwaltungsverfahren in Deutschland führen, ein oder mehrere nicht-sprechende Identifier, die keine personenbezogenen Elemente enthalten, vergeben und in den dezentralen Fachregistern der geführten Verwaltungsverfahren gespeichert.
2. Es wird ein Identitätsregister eingerichtet, das möglichst auf vorhandene Strukturen der Steuer-ID aufbauen soll und somit eine doppelte Datenhaltung ausschließt.
3. Ungeachtet des Identitätsregisters bleibt die heutige dezentrale Registerstruktur der Innenverwaltung erhalten.
4. Die zur Identifikation erforderlichen Daten einer Person werden öffentlichen Stellen auf gesetzlicher Grundlage stets aktuell und in hoher Qualität im Identitätsregister bereitgestellt.
5. Es werden Qualitätssicherungsprozesse eingerichtet, die die Aktualität, Konsistenz und Validität der personenidentifizierenden Basisdaten im Identitätsregister sicherstellen.
6. Als Beitrag zu mehr Transparenz für die Bürgerinnen und Bürger soll ein Datenschutzcockpit eingerichtet werden, das ihnen eine einfache, transparente und zeitnahe Wahrnehmung ihrer Auskunftsrechte nach der Datenschutz-Grundverordnung ermöglicht.
7. Die besonderen Anforderungen der Register im Sozial- und Gesundheitsbereich werden berücksichtigt.

Weitere Prüfung bedarf die genaue Ausgestaltung der Identifier-Lösung, insbesondere die Frage, welche technischen und rechtlichen Gründe für oder gegen die Verwendung eines einzigen oder mehrerer bereichsspezifischer Identifier sprechen. Ausgangspunkt der insoweit noch ergebnisoffenen Überlegungen ist zunächst die Steuer-ID.

Anhang 2: MPK-Beschluss vom 5. Dezember 2019

Besprechung der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder am 5. Dezember 2019

TOP 3.2 Leitlinien für eine Modernisierung der Registerlandschaft

Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Länder fassen folgenden Beschluss:

1. Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Länder nehmen den Bericht des BMI über den Stand der Registermodernisierung zur Kenntnis.

2. Das Ziel einer Registermodernisierung kann nur auf der Grundlage einer funktionierenden behördenübergreifenden Zusammenarbeit beim Aufbau der gemeinsamen Registerarchitektur erreicht werden. Das BMI soll dabei in enger Abstimmung mit den betroffenen Ressorts als zentraler Ansprechpartner für die Klärung themenfeldübergreifender rechtlicher und inhaltlicher Fragen der Umsetzung fungieren.

3. Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Länder sind sich darüber einig, dass durch eine Registermodernisierung die Grundlagen für einen registerbasierten Zensus ab 2024 geschaffen werden. Da insbesondere die Angaben zum Gebäude- und Wohnungsbestand sowie zu Bildungsabschlüssen bislang nicht in Registern vorliegen, sind Möglichkeiten für den Aufbau neuer Register zu prüfen.

4. Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Länder setzen sich dafür ein, dass die erforderlichen gesetzgeberischen Maßnahmen für ein registerübergreifendes Identitätsmanagement zeitnah auch unter dem Aspekt der Datensicherheit und des Datenschutzes geprüft und vorgestellt werden.

5. Die Registermodernisierung bietet die Chance, die Transparenz der Datenverarbeitung durch öffentliche Stellen für Bürgerinnen und Bürger und Unternehmen zu erhöhen. Diese Funktion kann von einem zukünftigen Datenschutzcockpit wahrgenommen werden. Durch ein Unternehmensstammdatenregister werden Unternehmen zudem von bürokratischem Aufwand entlastet

Anhang 3: Kernbotschaften der im Ergebnis des Auftrags an McKinsey & Company entstandenen „Aufwandsschätzung für die Einführung eines registerübergreifenden ID-Managements“ vom 28. Februar 2020

Kernbotschaften der Aufwandsschätzung

Kontext

- Registerübergreifendes Identitätsmanagement ist eine zentrale Komponente der Registermodernisierung und erforderlich, um die Anforderungen von vereinfachter Kommunikation zwischen Behörden, Onlinezugangsgesetz (OZG), Registerzensus sowie „Single Digital Gateway“-Verordnung (SDG-VO) in den kommenden Jahren zu erfüllen.
- Im Rahmen des IMK-Vorhabens zum registerübergreifenden Identitäts-management wurden seitens der Koordinierungsstelle für IT-Standards (KoSIT) und der Föderalen IT-Kooperation (FITKO) zwei mögliche Modelle in Abgrenzung zum sog. „Basismodell“ entwickelt – (1) die Nutzung der Steuer-ID als einheitlichen und zentralen Identifier in einer Architektur gemäß des „4-Corner-Prinzips“ (zID-Modell) sowie (2) die Erstellung neuer bereichs-spezifischer Identifier (bID-Modell).
- Um die beiden Modelle hinsichtlich der zu erwartenden finanziellen und zeitlichen Aufwände bei Einführung und Betrieb zu vergleichen, hat das Ministerium des Innern, für Bau und Heimat die Unternehmensberatung McKinsey & Company mit der Erstellung einer groben Aufwandsschätzung beauftragt, die hiermit vorgelegt wird.
- Die Annahmen für die Aufwandsschätzung basieren auf bekannten Daten-punkten aus dem bisherigen System der Steuer-ID, auf Vergleichswerten aus dem In- und Ausland sowie auf Experteneinschätzungen zur Herleitung und Validierung dieser Annahmen mit Vertretern mehrerer Bundesbehörden sowie weiteren relevanten technischen und fachlichen Akteuren.
- Die vorliegende Aufwandsschätzung ist **nicht** zu verstehen als:

- › Handlungsempfehlung für oder wider eines der betrachteten Modelle
- › Einschätzung aller sich ergebenden Aufwände im Kontext der Registermodernisierung (sondern nur jener, die unmittelbar einem Identifier zuzuordnen sind – auf Basis der verfügbaren Faktenlage)
- › Juristische Bewertung hinsichtlich rechtlicher Eignung der beiden Modelle, insbesondere nicht hinsichtlich der Erfüllung datenschutzrechtlicher Erfordernisse

Vergleich der Modelle und Vorgehen der Aufwandsschätzung

- Beide Modelle (zID-Modell und bID-Modell) müssen jeweils vier zentrale Anforderungen erfüllen:
  - › Eindeutige registerübergreifende Zuordnung von Datensätzen
  - › Etablierung wirksamer Sicherungsmaßnahmen zur Verhinderung einer Profilbildung
  - › Sicherstellen der Nachvollziehbarkeit des entstehenden Datenaustauschs
  - › Einfache Umsetzung innerhalb der Bestandsarchitektur mit Flexibilität für Änderungen.
- Die Modelle wurden im Rahmen dieser Betrachtung auf Basis dieser Annahmen weiter konkretisiert, um eine Vergleichbarkeit zu ermöglichen. Insbesondere wurde davon ausgegangen, dass als Sicherungsmaßnahme in beiden Modellen die besondere Überwachung sowie der besondere Schutz der Datenübertragung selbst erforderlich ist. Dafür bietet sich das „4-Corner-Prinzip“ an, welches z.B. in der Innenverwaltung und im Sozialbereich bereits in entsprechender Architektur vorliegt, die allerdings stellenweise ertüchtigt werden muss.
- Die anfallenden finanziellen und zeitlichen Aufwände (sowohl einmalig als auch laufend) wurden für beide Modelle in drei Aufwandsmodule unterteilt, nämlich:
  - › Die Erstellung der neuen Identifier (nur bID-Modell) sowie die Zuspielung dieser in alle vorrangigen personenbezogenen Register unter Sicherstellung der Datenkonsistenz;
  - › den Aus- bzw. Aufbau eines „ID-Registers“ aufbauend auf der bestehenden Steuer-ID-Datenbank (zID-Modell) bzw. als separate neue Stelle (bID-Modell) unter Berücksichtigung des notwendigen Personals, Materials sowie der benötigten IT-Infrastruktur und -dienstleistungen;
  - › den Aufbau von Infrastruktur- und Kommunikationskomponenten in den beteiligten Stellen und Registern, insbesondere die notwendige Anpassung von Fachverfahren, den Aufbau von „Gateways“ zwischen Sektoren und die Erweiterung des bestehenden Rechtemanagements.

- Das bID-Modell sieht eine zusätzliche Sicherungsmaßnahme – die der Bereichsspezifität des Identifiers - vor, woraus sich über das zID-Modell hinaus konsequenterweise drei Kernunterschiede und zusätzliche Aufwände ergeben:

  › Vollständige organisatorische, technische und ggf. physische Trennung des zentralen „ID-Registers“ von der Steuer-ID-Datenbank;

  › Zwingende Schaffung neuer, kryptographisch gesicherter Schnittstellen und Kommunikationskanäle zwischen allen vorrangigen (dezentralen) Fachverfahren/Register und dem „ID-Register“ in einem ersten Schritt;

  › Grundlegende Veränderung der bestehenden Netztopologie, die bisher auf bestimmten „Knoten“ wie etwa den Melderegistern oder der Rentenversicherung beruht, die als Datendrehscheiben agieren, und im bID-Modell eine solche Rolle nicht mehr unmittelbar bereichsübergreifend wahrnehmen können.

Ergebnisse der Aufwandsschätzung

- Für die Einrichtung und den Betrieb des zID-Modells ist mit einmaligen Kosten von 90 bis 145 Mio. EUR, laufenden Kosten von 5 bis 15 Mio. EUR sowie einer Umsetzungsdauer von drei bis sechs Jahren zu rechnen.

- Für die Einrichtung und den Betrieb des bID-Modells ist mit einmaligen Kosten von 170 bis 340 Mio. EUR, laufenden Kosten von 20 bis 30 Mio. EUR sowie einer Umsetzungsdauer von sieben bis zehn Jahren zu rechnen.

Einordnung der Ergebnisse

- Die ermittelten Aufwände fokussieren sich auf die Inbetriebnahme eines registerübergreifenden Identitätsmanagements im Rahmen eines Anschlusses von 26 als vorrangig identifizierten Registern und berücksichtigt daher nicht darüber hinaus gehende Aufwände, nämlich z.B.:

  › Anschluss weiterer (nachrangiger) personenbezogener Register oder registerähnlicher Datenbanken;

  › Anschluss dezentraler öffentlicher Akteure, wie etwa auf kommunaler Ebene (Schul- und Gesundheitsbehörden, Polizeien, Jugendämter);

  › Anschluss dezentraler privatwirtschaftlicher Akteure, wie etwa aller Arbeitgeber, Banken und Versicherungen

  › Weitere Aufwände im Kontext Registermodernisierung, die nicht unmittelbar zur Einführung eines registerübergreifenden Identitätsmanagements notwendig sind, z.B. die Bereinigung von Registern oder die Ertüchtigung von bisher nicht bereichsübergreifend erreichbaren Registern.

- Im Fall des bID-Modells wäre zu erwarten, dass diese vorangehend genannten Aufwände höher ausfallen als bei der Umsetzung des zID-Modells, da hier eine komplexere Netztopologie vorliegt, die Funktion bestehender „Knoten“ wie etwa der Meldebehörden nur noch eingeschränkt nutzbar wäre und zudem davon ausgegangen wird, dass in allen Systemen, die bisher die Steuer-ID nutzen (z.B. bei Banken, Versicherungen und Arbeitgebern), diese durch die Finanz-bID ersetzt werden müsste.

- Die nötige umfangreiche Anpassung der Fachverfahren stellt einen signifikanten quantifizierten Aufwandstreiber im bID-Modell dar. Die Zahl betroffener Fachverfahren wird zwischen 300-650 geschätzt, kann aber je nach Zahl einbezogener Register und Leistungen höher ausfallen. Je 100 weiterer anzupassender Fachverfahren würden sich die Aufwände im bID-Modell um 18 bis 28 Mio. EUR und im zID-Modell um 1,5 bis 4 Mio. EUR erhöhen.

- Das zID-Modell sieht im Konzeptpapier vor, dass der Betrieb eines registerübergreifenden Identitätsmanagements basierend auf dem bestehenden „4-Corner-Prinzip“ möglich ist. Falls in Zukunft entschieden werden sollte, dass hierfür für viele oder alle Fachverfahren eine Ende-zu-Ende-Verschlüsselung bis hinein ins Fachverfahren bzw. den Arbeitsplatz nötig ist, würde dies für eine Vielzahl von Fachverfahren auch in diesem Modell eine Ertüchtigung erforderlich machen, welche mit signifikanten Kosten verbunden wäre. Da eine solche Ertüchtigung jedoch nicht Teil der zugrundeliegenden Konzeptpapiere ist, werden diese Aufwände in der Aufwandsschätzung nicht betrachtet (siehe auch Box 6).

- Die aktuellen Planungen sehen vor, dass im bID-Modell nach einer zu definierenden Übergangszeit die Nutzung bestehender Identifier, wie etwa der Steuer-ID, nicht mehr zulässig wäre und somit alle vorangehend genannten Akteure eine direkte Anbindung an das „ID-Register“ benötigen und existierende, bereichsübergreifende Kommunikationsverbindungen angepasst werden müssten. Über die Höhe solcher Aufwände kann zum jetzigen Zeitpunkt aufgrund mangelnder Datenlage über Anzahl und Komplexität der anzupassenden Systeme keine exakte Aussage getroffen werden.

- Die niedrigeren erwarteten Aufwände im Fall des zID-Modells und die im Falle des bID-Modells vorhandene zusätzliche Sicherungsmaßnahme werden neben

weiteren Faktoren im Fortgang der politischen Entscheidungsfindung für ein präferiertes Modell gegeneinander abzuwägen sein.

Anlage: Zwei Modelle für das Registerübergreifende Identitätsmanagement (separate Anlage)

Diese – aufgrund des Umfangs - separate Anlage und eigene Datei trägt die Bezeichnung „Anlage IMK-Abschlussbericht Modelle für das Registerübergreifende Identitätsmanagement“.

Bundesministerium
des Innern, für Bau
und Heimat

Anlage

IMK-Abschlussbericht
Modelle für das Registerübergreifende Identitätsmanagement

zum

Abschlussbericht

zur Sondierung eines
registerübergreifenden Identitätsmanagements
mit Einbezug der Erfahrungen mit der Steuer-Identifikationsnummer
für die Innenministerkonferenz
17. - 19. Juni 2020

Mögliche Modelle und Lösungsvarianten für bereichsspezifische Personenkennzeichen in Deutschland

Betrachtung im Rahmen der Unterarbeitsgruppe von EG 1 / EG 2 des IMK Vorhabens zur Registermodernisierung

Unteruntertitel

Version: 1.0

Stand: 08.01.2020

Version	Datum	Autor	Aktion
0.5	13.12.2019	Hoose	Erstellung des ersten Entwurfs
0.6.	30.12.2019	Rockmann, Gellner	Kommentierung und Ergänzungen
0.8	06.01.2019	Hoose	Übernahme der Änderungen und Kommentare. Fertigstellung fehlender Abschnitte
0.9	07.01.2019	Rockmann, Gellner	Anmerkungen und Überarbeitungen
1.0	08.01.2019	Hoose	Fertigstellung des Dokuments

Inhaltsverzeichnis

Zentrale Begriff und Synonyme

Begriff	Erläuterung	Synonyme
Tätigkeitsbereich	In Österreich werden die Gültigkeitsbereiche für bereichsspezifische Kennzeichen (bPK) als Tätigkeitsbereiche bezeichnet. Diese können fachliche Bereiche (bspw. Steuer) oder auch fachunabhängige oder tätigkeitsübergreifende Gültigkeitsbereiche (Personalverwaltung, Datenschutz) definieren. Dieser Begriff wird auch im vorliegenden Dokument genutzt, wenn über die fachliche Aufteilung der bereichsspezifischen Kennzeichen gesprochen wird. Im Rahmen der EGs wird in diesem Kontext auch von Sektoren gesprochen.	Sektor, Bereich
ID-Register	Mit dem Begriff ID-Register wird das technisch-organisatorische System zur Generierung, Aufbewahrung und Bereitstellung der bPKs bezeichnet. In diesem System erfolgt auch die Aufbewahrung eines Datenkranzes, der die eindeutige Abfrage mittels Stammdaten einer natürlichen Person bzw. die Abfrage eines aktuellen Stammdatensatzes einer natürlichen Person ermöglicht.	Registerbehörde, ID-Registersystem
Register	Ein elektronisches oder papiergebundenes System mit Daten über bestimmte Sachverhalte wie natürliche oder juristische Personen, Grundstücke oder auch Umweltinformationen (siehe OECD: A set of files (paper, electronic, or a combination) containing the assigned data elements and the associated information. – OECD definition).	Kernregister
Fachverfahren	Elektronische Verfahren bzw. fachliche Software zur Unterstützung der Fallbearbeitung in einem Verwaltungsverfahren innerhalb der zuständigen Stelle.	
Onlinedienst	Elektronische Systeme für Antragssteller oder berichtspflichte Personen und Organisationen, um verfahrensinitiierende Daten zu erfassen und nachgelagerte Systeme der Verwaltung (bspw. Fachverfahren oder E-Akte Systeme) zu übergeben.	Onlineantrags-dienst

Anfragende Behörde	Behörde mit einem Interesse an Daten oder Sachverhaltsauskünften einer anderen Behörde oder eines Kernregisters.	Ersuchende Behörde
Angefragte Behörde	Registerführende oder verfahrensbeteiligte Behörde, die einer anfragenden Behörden Daten oder Sachverhaltsauskünfte aus ihrem Datenbestand übermittelt.	Zielbehörde, Auskunfts-erteilende Behörde

1 Umfang der vorliegenden Betrachtung

Die vorliegende Betrachtung soll lediglich erste Vorschläge und Konkretisierung für ein Modell bereichsspezifischer Personenkennzeichen (bPK) für Deutschland erarbeiten. Sie ist keine abschließende verfassungsrechtliche und datenschutzrechtliche Bewertung im Rahmen der Fragestellung.

Die erarbeiteten Vorschläge sollen eine Basis bieten, um den Ansatz des bereichsspezifischen Personenkennzeichens mit dem Ansatz eines einheitlichen Personenkennzeichens auf Basis einer detaillierten Anforderungsbetrachtung, rechtlicher Bewertungen, Risikobetrachtungen und Analysen möglicher Architekturansätze zu vergleichen.

2 Darstellung eines denkbaren bPK Modells in Deutschland

2.1 ID-Register: Funktionsumfang und Rolle im bPK Modell

Voraussetzung für ein bPK-Modell ist ein zentrales ID-Register, welches die folgenden Aufgaben hat:

- Berechnung der Stammzahl und der daraus abgeleiteten bPKs
- Bereitstellung der bPKs auf Anfrage an einen Berechtigten
- Bereitstellung eines verschlüsselten bereichsfremden bPK (oder einer alternativen Methode) an einen Berechtigten zur Kommunikation mit einer Behörde eines anderen Bereichs
- Abruf von Daten aus dem Datenkranz des ID-Registers durch alle berechtigten Stellen unter Angabe des bPK

2.2 Berechnung der Stammzahl und bPKs

Es wird vorgeschlagen, dem grundlegenden Modell aus Österreich zur kryptografischen Berechnung des bPK aus einer Stammzahl zu folgen, da dort langjährige Erfahrungen hinsichtlich der Sicherheit und technischen Umsetzung des Verfahrens vorhanden sind. Von diesen Erfahrungen kann Deutschland im Rahmen eines technischen und organisatorischen Aufbaus des ID-Registers profitieren und diese Ergebnisse nachnutzen.

Auf dieser Basis würden in Deutschland die wesentlichen Schritte zur Erstellung eines bPK wie folgt ablaufen:

- Ausgangspunkt ist die Steuer-ID, da die Datenbank des BZSt die notwendigen Qualitätsanforderungen erfüllt.
- Aus der Steuer-ID wird mittels kryptografischer Verfahren eine eindeutige Stammzahl berechnet, die im ID-Register nicht gespeichert wird (siehe 2.3). Eine Rückberechnung der Steuer-ID aus der Stammzahl ist für Dritte nicht möglich.
- Aus der Stammzahl wird mit einem weiteren kryptografischen Verfahren für jeden definierten Tätigkeitsbereich eine zugehörige bPK berechnet. Ausgehend von eines bPK ist weder eine Rückrechnung auf die Stammzahl noch die Berechnung eines bPKs eines anderen Tätigkeitsbereichs möglich. Die vorherige Berechnung der Stammzahl stellt eine weitere Sicherheitsmaßnahme dar, damit kein direkter Zusammenhang zwischen den abgeleiteten bPKs mit der allgemein bekannten Steuer-ID besteht.

Die hier aufgezeigten Berechnungsschritte würden grundsätzlich immer dann angestoßen werden, wenn eine neue Steuer-ID bspw. aufgrund einer Geburt oder eines Zuzugs aus dem Ausland generiert wird. Eine Veranschaulichung dieses Vorgehens ist der Abbildung 1 zu entnehmen.

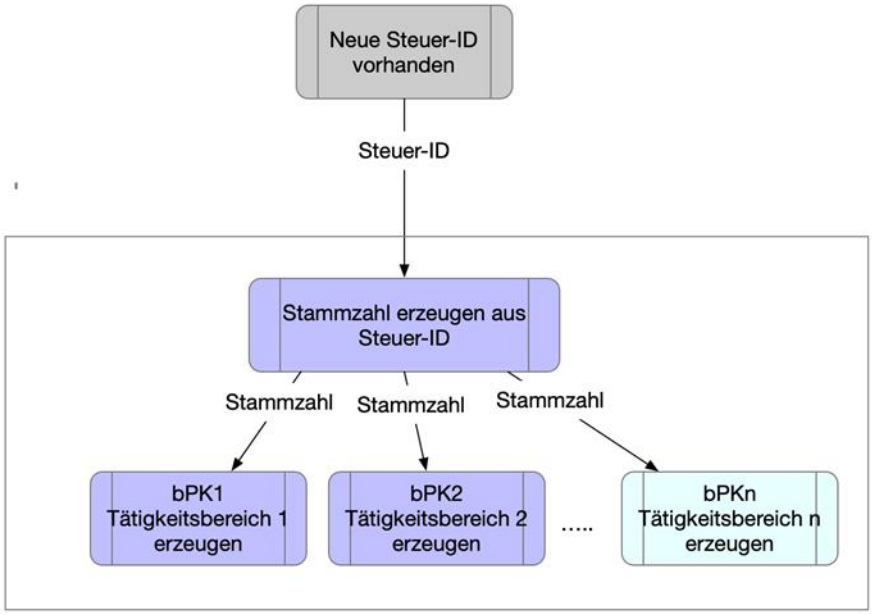


Abbildung 1 Berechnungsschritte des bPK auf Basis der Steuer ID

2.3 Lösungsvarianten zur Referenzierung auf bereichsfremde bPKs

Um einen Datenaustausch automatisiert durchzuführen, muss im angefragten Datenbestand eine eindeutige und korrekte Zuordnung der durch den Anfragenden übermittelten Daten zu einem Datensatz im Bestand des Angefragten möglich sein.

Innerhalb eines Tätigkeitsbereiches wird das durch das bPK und ein weiteres übermitteltes Datum sichergestellt.

Überschreitet der Datenaustausch jedoch die Grenze eines Tätigkeitsbereichs, wird über das ID-Register dem Anfragenden das verschlüsselte bPK des anderen Tätigkeitsbereichs oder eine gleichwertige Referenz verschlüsselt übermittelt.

Hierzu sind die folgenden beiden Lösungen denkbar:

Lösungsvariante 1: Austausch mittels verschlüsselter bereichsfremder bPKs

Das ID-Register stellt einer berechtigten anfragenden Behörde das gewünschte bereichsfremde bPK bereit, welches mittels des öffentlichen Schlüssels der Zielbehörde für den Datenaustausch verschlüsselt wird. So kann nur die Zielbehörde das bPK entschlüsseln. Dieses Modell entspricht weitestgehend dem österreichischen Modell. Für die Schlüsselverwaltung können vorhandene Public Key Infrastrukturen der öffentlichen Verwaltung (wie bspw. DVDV oder SAFE) genutzt werden.

Lösungsvariante 2: Austausch mittels eindeutiger temporärer IDs aus dem ID-Register

Das ID-Register stellt der anfragenden Behörde eine temporär gültige UUID (Universally Unique Identifier[1]) für das gewünschte bereichsfremde bPK der Zielbehörde bereit. Diese UUID wird durch das ID-Register für diese konkrete Anfrage erzeugt und temporär mit dem dazugehörigen bPK der Zielbehörde in einem internen Systemeintrag verknüpft und gespeichert.

Die anfragende Behörde übermittelt im Rahmen des Datenaustauschs die UUID an die Zielbehörde. Die Zielbehörde fragt schließlich mit dieser UUID das dazugehörige bPK ihres Tätigkeitsbereichs beim ID-Register ab. Danach oder nach einem zu definierenden Zeitraum ohne Abfrage wird die UUID aus dem Datenbestand des ID-Registers gelöscht.

[1] Siehe https://de.wikipedia.org/wiki/Universally_Unique_Identifier. Andere weitestgehend kollisionsfreie IDs wären für den vorliegenden Vorschlag genauso denkbar.

Vergleichende Bewertung der Lösungsvarianten

Beide Lösungsvarianten ermöglichen prinzipiell einen automatisierten Datenaustausch. Bei Lösungsvariante 1 könnte für die Implementierung auf Erfahrungen aus Österreich zurückgegriffen werden. Ein weiterer Vorteil besteht darin, dass nach dem initialen Abruf des verschlüsselten bPK des Fremdbereichs keine weitere Kommunikation mit den ID-Registern durch den zweiten Kommunikationspartner notwendig ist, da das betreffende bPK sowie der private Schlüssel bei der Zielbehörde bereits vorhanden sind.

Im Gegensatz hierzu erzwingt der Einsatz einer temporär gültigen UUID in der Lösungsvariante 2, dass auch der zweite Kommunikationspartner mit dem ID-Register kommunizieren muss, um das betreffende bPK mit der UUID beim ID-Register zu erfragen. Dies ist ein weiteres Hemmnis im Hinblick auf die missbräuchliche Nutzung – zum einen aufgrund der nur temporären Gültigkeit der UUID und zum anderen aufgrund der Kontrollmöglichkeit an einer zentralen Stelle unabhängig vom Transportverfahren. Auch wäre die für Lösungsvariante 1 notwendige PKI Infrastruktur in dieser Lösungsvariante nicht in gleichem Umfang erforderlich, da den Kommunikationspartner lediglich eine UUID bereitgestellt wird. Gleichzeitig würde aber aufgrund der zentralen Rolle des ID-Registers die Kritikalität des ID-Registers sowie Last- und Verfügbarkeitsanforderungen an die Kommunikationsinfrastruktur steigen, wodurch vermutlich auch die technische Komplexität höher als bei Lösungsvariante 1 ausfallen würde.

Eine abschließende Bewertung müsste jedoch in einer Folgeuntersuchung geklärt werden. Daher werden beide Lösungsvarianten vorläufig als mögliche Lösungen für ein deutsches bPK Modell bewertet.

2.4 Tätigkeitsbereiche für die Aufteilung der bPKs

Bereichsspezifische PKs sehen wie in Österreich die Abgrenzung von fachlichen Tätigkeitsbereichen (Sektoren) vor. Allerdings erscheint eine - im Vergleich zu Österreich mit 35 abgegrenzten Bereichen - wesentlich verringerte Anzahl als ausreichend, um die damit verbundenen Datenschutzziele zu erreichen. Eine konkrete Festlegung der Bereiche wird in diesem Papier nicht vorgesehen. Es wird aber davon ausgegangen, dass eine Zahl von 10 bis höchstens 20 Bereichen ausreichend ist.

2.5 bPKs für übergreifende Anwendungen

Neben bPKs für fachliche Tätigkeitsbereiche wird zusätzlich vorgeschlagen, bPKs für zwei übergreifende Anwendungsfälle zu bilden:

- Bürger-bPK für Bürgerkonten (Nutzerkonto im Sinne des OZG)
- Datenschutz-bPK für ein Datenschutz Cockpit

2.5.1 Bürger-bPK für Bürgerkonten

Gemäß § 2 Absatz 5 des OZG werden Nutzerkonten als dauerhaftes Identifikationssystem für Nutzer definiert und sollen einen Zugriff auf staatliche Dienste gewähren. Für natürliche Personen existieren hierfür sogenannte Bürgerkonten.

Es wird vorgeschlagen, für die Bürgerkonten eine Bürger-bPK vorzusehen, die nur im Bürgerkonto und im ID-Register gespeichert werden darf. Alleiniger Zweck dieser Bürger-bPK ist es, dass ein Bürgerkonto aus dem ID-Register automatisiert verschlüsselte bPK Referenzen abrufen kann, um im Rahmen von OZG-Leistungen Daten und Nachweise abzurufen. Dieses Datenaustauschszenario wird in Abschnitt 3.2 vertieft dargestellt.

2.5.2 Datenschutz-bPK für das Datenschutz-Cockpit

Mit einem Datenschutz-Cockpit soll für den Bürger eine erhöhte Transparenz hergestellt werden, indem für ihn nachvollziehbar ist, welche Daten zwischen Behörden ausgetauscht worden sind. Ein Datenschutz-bPK kann eine Möglichkeit bieten, die im konkreten Datenaustausch zwischen Behörden relevanten Metadaten automatisiert im Datenschutz-Cockpit bereitzustellen.

Eine Referenz auf das Datenschutz-bPK könnte grundsätzlich in jeglicher Kommunikation mitgeführt werden und dem Datenschutz-Cockpit eine Erfassung der Metadaten des Datenaustauschs über die Transportverfahren ermöglichen. Die Referenz auf das Datenschutz-bPK würde eine anfragende Stelle im Rahmen der Abfrage des fachlichen bPK vom ID-Register miterhalten.

Weil nur die Referenz auf das Datenschutz-bPK außerhalb des Datenschutz-Cockpits genutzt wird, würde das eigentliche Datenschutz-bPK keine Verknüpfungen zu Register- und Stammdaten eines Bürgers aufweisen. Innerhalb des Datenschutz-Cockpits wären jedoch in einem erheblichen Umfang Metadaten zum Datenaustausch von Bürgerdaten mit dem jeweiligen Datenschutz-bPK verbunden.

Die Meldung der Metadaten und der Datenschutz-bPK Referenz an das Cockpit könnte je nach Lösungsvariante und Risikobetrachtung entweder durch die jeweiligen fachlichen Kommunikationspartner, die Transportverfahren (bspw. bei einer Four-Corner Architektur wie OSCI), das ID-Register oder mehrere Stellen parallel erfolgen. Eine Übersicht der möglichen Übergabepunkte ist in der folgenden Abbildung dargestellt.

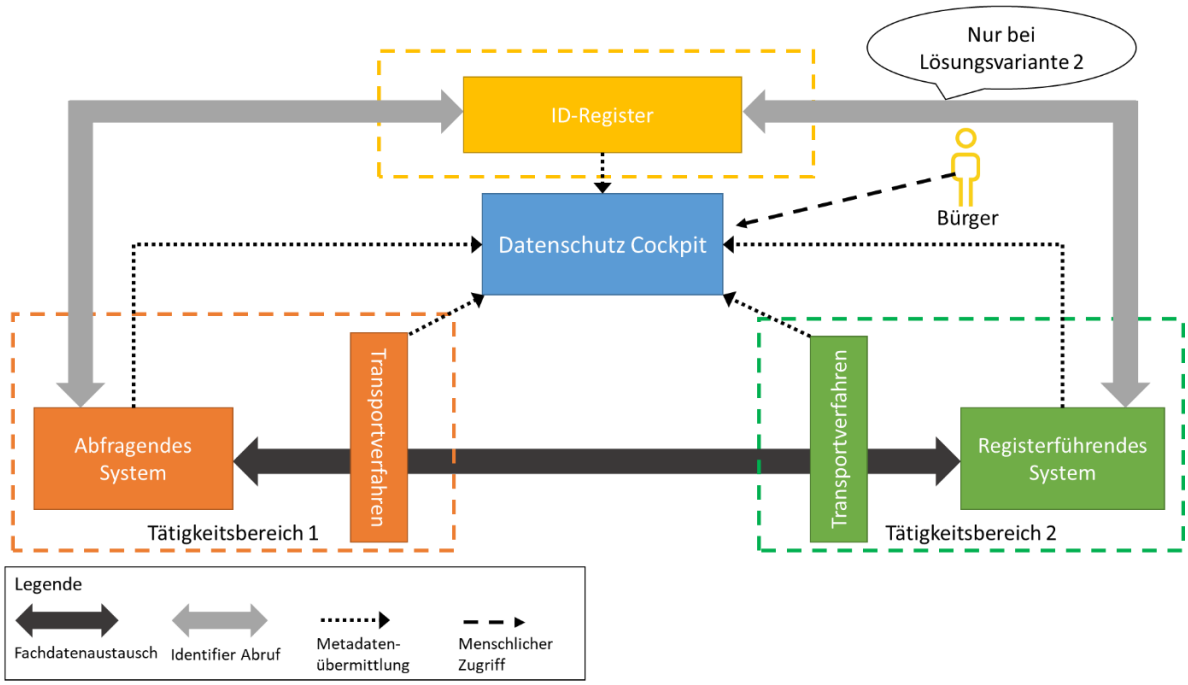


Abbildung 2 Übersicht von Übermittlungspunkten an ein Datenschutz-Cockpit

2.6 Bereitstellung des bereichseigenen bPK an die Datenbestände der Verwaltung

Der grundsätzliche Datenfluss bei der Errechnung und der Verteilung des bereichseigenen bPKs wird in der folgenden Abbildung dargestellt.

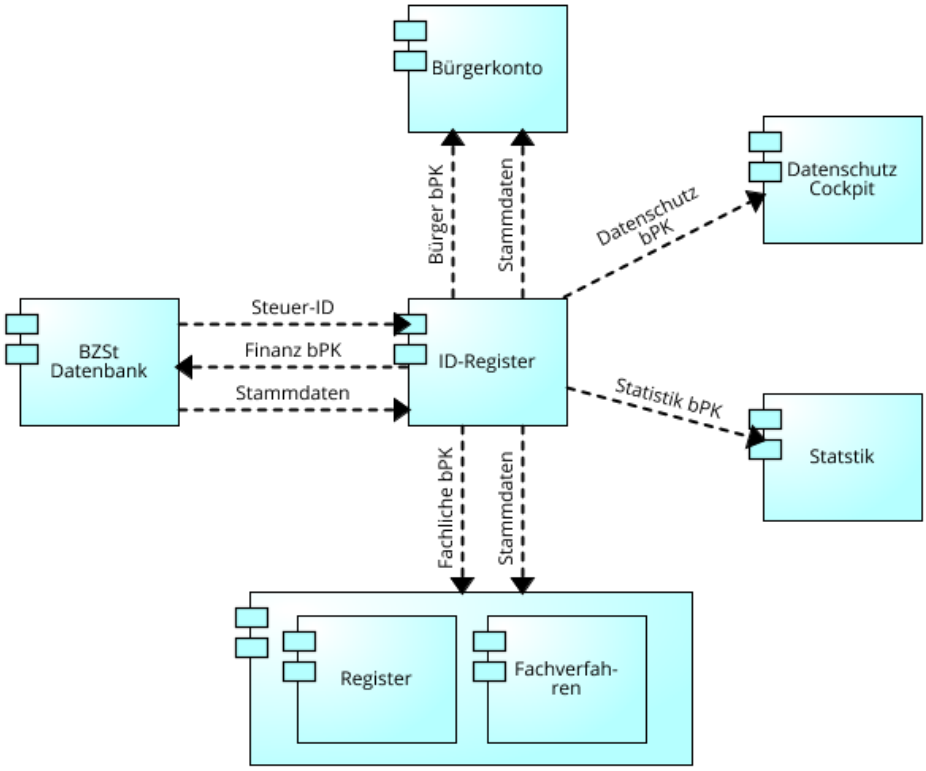


Abbildung 3 Datenfluss im Rahmen der bPK Berechnung und Verteilung

Wie diese bPKs konkret in die Datenbestände der Register und Fachverfahren übertragen werden können, wird für die Einführungsphase und den Regelbetrieb des ID-Registers in den Folgeabschnitten näher erläutert.

2.6.1 Bereitstellung von bPKs bei der Einführung des bPK-Systems in Deutschland

Für definierte Kernregister der Verwaltung[2] sollten das bPK des zugehörigen Tätigkeitsbereichs verpflichtend flächendeckend anlasslos ausgrollt werden, da beim Ausrollen und während der Einführungsphase mit Klärungsaufwand zu rechnen ist.

Für alle anderen Register ist die bedarfsbezogene bPK Übermittlung vorgesehen, d.h. für bereits abgeschlossene Verfahren werden bPKs nicht mehr nachträglich abgerufen und gespeichert.

[2] Eine solche Definition existiert aktuell in Deutschland nicht. (Siehe Abschnitt 4.3)Diese würde jedoch den identifizierten bestehenden Registern der DeSTATIS Untersuchung im NKR Gutachten entsprechen sowie zukünftig notwendigen Registern gemäß dem NKR Gutachten entsprechen.

2.6.2 Automatische Verteilung bei neuen Einträgen in der BZSt Datenbank

Sollten neue Einträge entstehen, weil bspw. eine Geburt in einem Melderegister verzeichnet wurde oder ein Zuzug aus dem Ausland erfolgt ist, sollten diese direkt an folgende Stellen übermittelt werden:

- **Bundeszentralamt für Steuern:** Das Finanz-bPK an die BZSt Datenbank einschließlich der Personenstammdaten für eine eindeutige Zuordnung des bPK zum Personeneintrag
- **Ausländerzentralregister: Das** Innenverwaltung-bPK einschließlich der Personenstammdaten für eine eindeutige Zuordnung des bPK zum Personeneintrag
- **Meldewesen:** Das Innenverwaltung-bPK an die zuständige Meldebehörde einschließlich der Personenstammdaten für eine eindeutige Zuordnung des bPK zum Personeneintrag

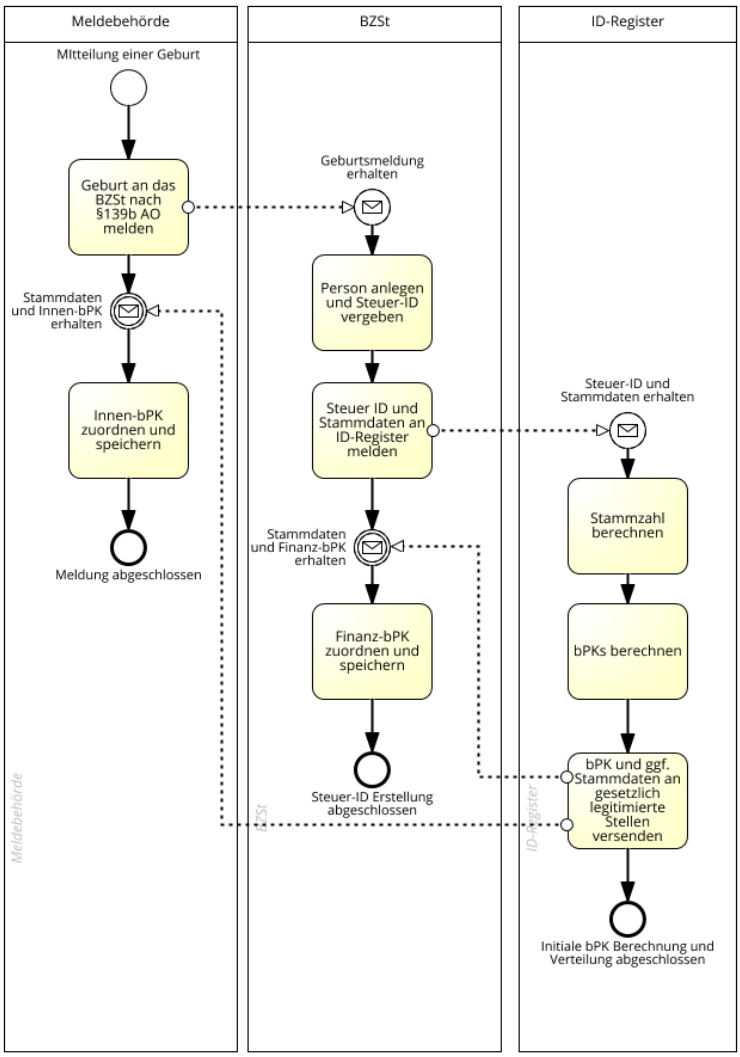


Abbildung 4 Initiale Berechnung und Verteilung der bPKs bei der Geburtsmeldung

Eine automatisierte Übertragung der bPKs direkt nach Berechnung an diese Stellen wird vorgeschlagen, um den Gesamtprozess zu vereinfachen und eine Eindeutigkeit der Daten schon nach dem Entstehen dieser Daten im jeweiligen Fachprozess zu gewährleisten. Für alle weiteren Register ist ein Abruf des bereichseigenen bPK im Rahmen eines konkreten Verwaltungsverfahrens ausreichend, wenn der Personeneintrag tatsächlich entsteht (bspw. bei der Anmeldung eines KFZ).

3 Betrachtung der Datenaustauschszenarien mittels bPKs

Der Fokus des einheitlichen PK wie auch des bPK liegt darauf, den automatisierten Datenaustausch von Datensätzen zu natürlichen Personen zu ermöglichen. Automatisiert bedeutet in diesem Kontext, dass ein Datensatz einer natürlichen Person im Normalfall ohne manuelle Klärung (bspw. aufgrund von Mehrfachtreffern) ausgetauscht werden kann. Im Folgenden werden zwei Grundszenarien betrachtet, bei denen ein bPK funktionieren muss:

- Datenaustauschszenario 1: Datenabruf durch Behörden aus Registern oder sonstigen Datenbeständen
- Datenaustauschszenario 2: Datenabruf im Rahmen der Antragsstellung zur Vorbefüllung von Anträgen oder Beifügen amtlicher Nachweise

Im Rahmen der vorliegenden Abschnitte werden diese Szenarien und der Einsatz des bPK kurz erläutert und anhand einer Prozessdarstellung visuell veranschaulicht. Im Rahmen der Prozessdarstellung werden Verschlüsselungsaspekte nicht explizit veranschaulicht, um die Lesbarkeit der Prozessmodelle zu vereinfachen. Für die Verschlüsselung der bPKs bzw. bPK-Referenzen gelten für die jeweiligen Lösungsvarianten folgende Grundsätze:

- Lösungsvariante 1: Bereichseigene bPKs werden bei einer Anfrage beim ID-Register mit dem Schlüssel der anfragenden Stelle verschlüsselt. Bereichsfremde bPKs werden mit dem Schlüssel der Zielbehörde durch das ID-Register verschlüsselt.
- Lösungsvariante 2: Bereichseigene bPKs werden bei einer Anfrage beim ID-Register mit dem Schlüssel des ID-Register durch die anfragende Stelle verschlüsselt. Das der UUID zugehörige bPK wird durch das ID-Register verschlüsselt übersendet.

3.1 Datenabruf aus Registern oder sonstigen Datenbeständen durch Behörden

In diesem Datenaustauschszenario ruft eine Behörde im Rahmen einer gesetzlichen Erlaubnis oder aufgrund einer Einwilligung des Antragsstellers Daten zu einer natürlichen Person bei einer Behörde mit anderem Tätigkeitsbereich elektronisch ab.

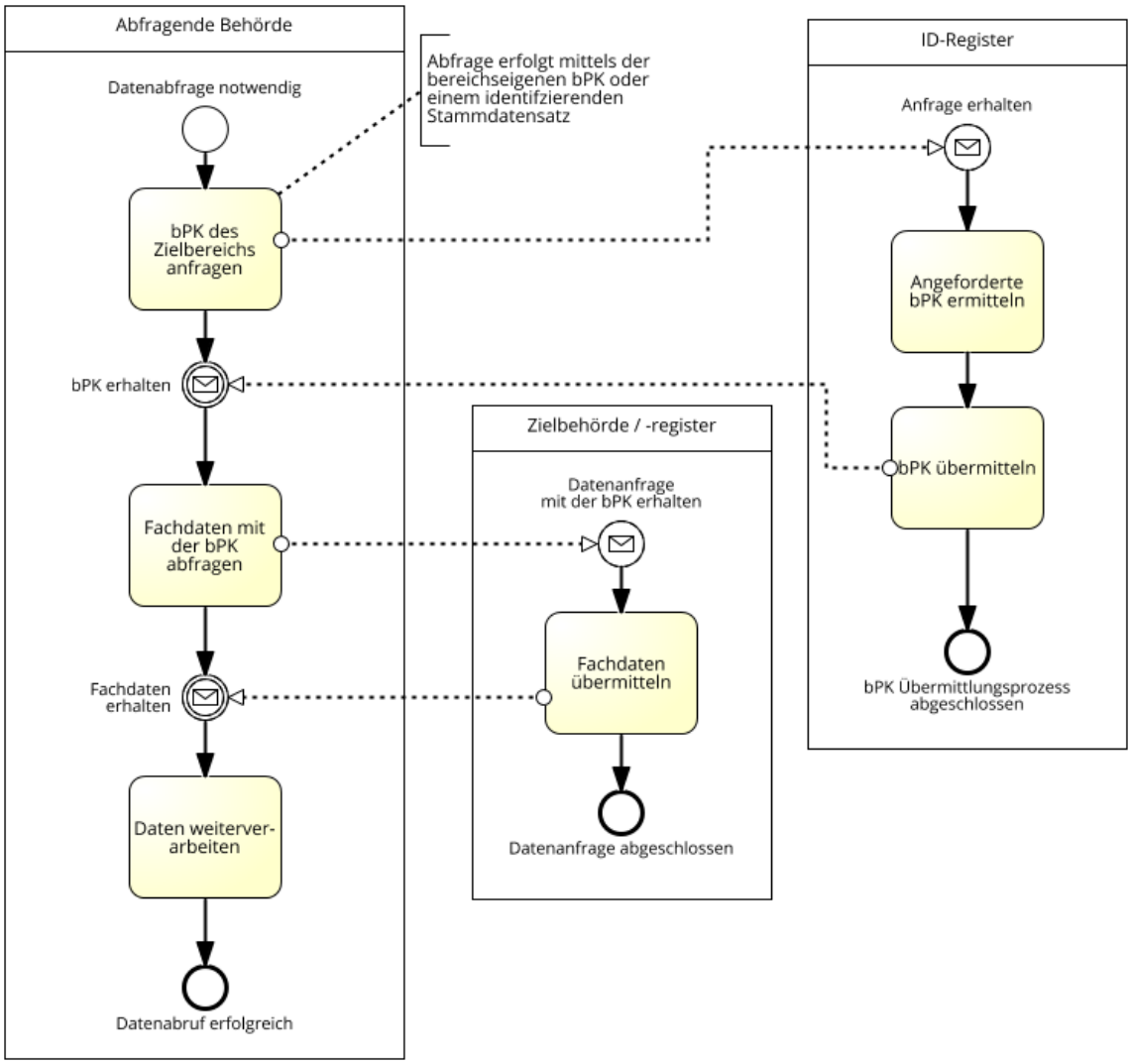


Abbildung 5 Datenaustauschszenario 2: Datenabruf aus Registern oder sonstigen Datenbeständen durch Behörden (Lösungsvariante 1 mit verschlüsseltem Fremdbereichs-bPK)

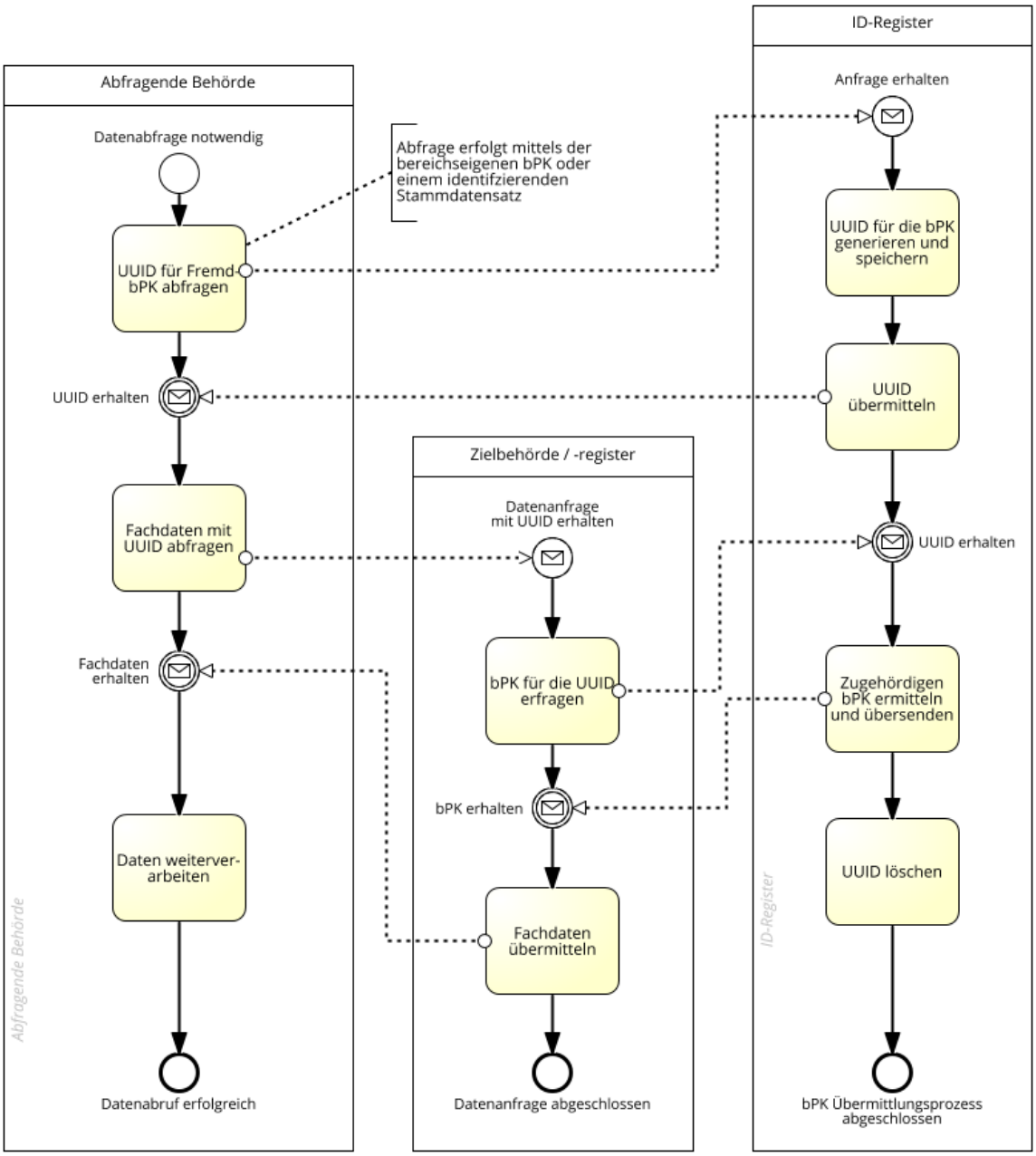


Abbildung 6 Datenaustauschszenario 2: Datenabruf aus Registern oder sonstigen Datenbeständen durch Behörden (Lösungsvariante 2 mit UUID)

3.2 Datenabruf im Rahmen der Antragsstellung nach OZG

In diesem Datenaustauschszenario ruft ein Nutzer mit einem Onlineantragsdienst Daten aus einem behördlichen Datenbestand ab, um mit diesen Daten das Antragsformular zu befüllen.

In diesem Datenaustauschszenario wird davon ausgegangen, dass der Onlinedienst über eine Schnittstelle das verschlüsselte bPK oder die UUID des Zieltätigkeitsbereichs beim Bürgerkonto

anfordert und das Bürgerkonto[3] dann den Abruf der hierfür notwendigen bPK Referenzen beim ID-Register übernimmt. Über diese technische und prozessuale Ausgestaltung wird gewährleistet, dass das Bürger-bPK nur innerhalb des Bürgerkontos und des ID-Registers gespeichert wird und kein direkter Zugriff von Onlinediensten auf das ID-Register möglich ist.

Anders als bei dem vorherigen Szenario werden beim Datenabruf zur Befüllung von Formulardaten prinzipiell höhere Anforderungen an einen Identifier gestellt:

- Ein Datenabruf muss eindeutig und fehlerfrei sein, da bspw. eine Auswahl des korrekten Datensatzes aus einer Trefferliste durch den Antragsteller aus datenschutzrechtlichen und verfahrensrechtlichen Gründen ausgeschlossen ist.
- Der Datenabruf in einer solchen Situation muss in einer sehr kurzen Zeit im Hintergrund erfolgen, da komplexe Auswahlen und Wartezeiten von mehreren Minuten für eine Antragsstellung nicht hinnehmbar sind.

Die erhöhten Anforderungen werden nach der vorläufigen Einschätzung mit einem bPK genauso gewährleistet wie bei einem einheitlichen PK.

[3] Bzw. ein dem Bürgerkonto zugeordneter Registerabrufdienst. Die konkrete interne technische Implementierung ist für das Beispiel nicht relevant.

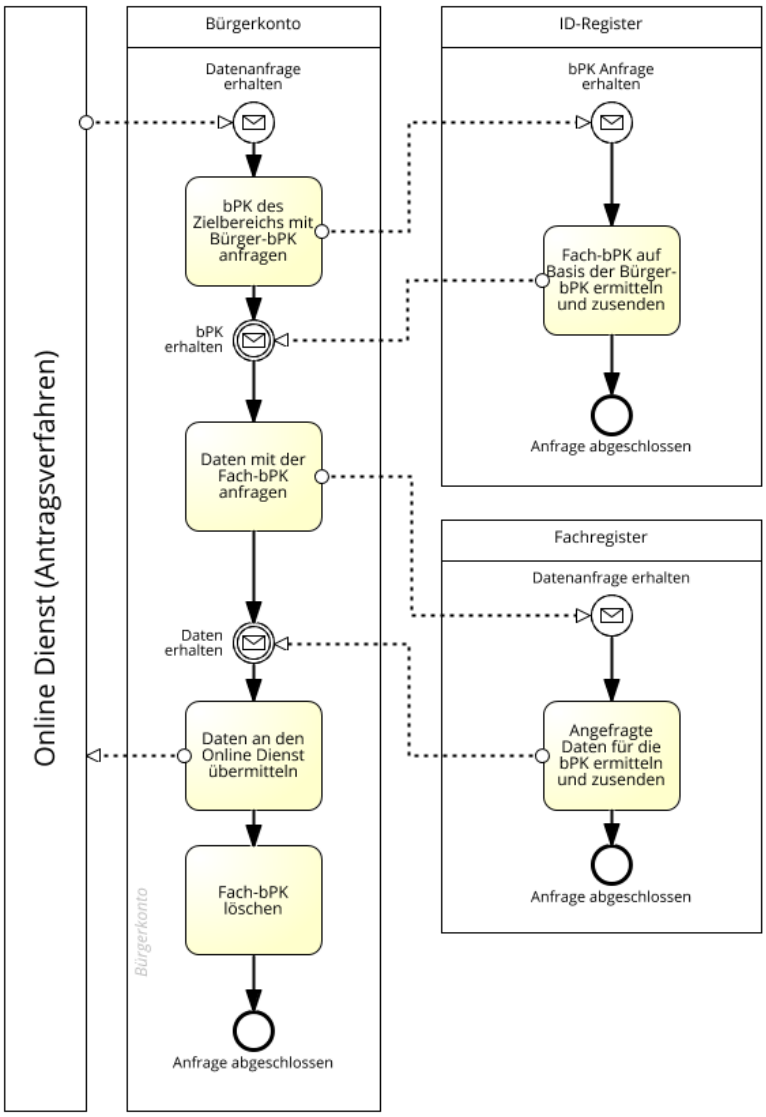


Abbildung 7 Datenaustauschszenario 2: Datenabruf während der Antragsstellung im Rahmen von Antragsverfahren nach OZG (Lösungsvariante 1 mit verschlüsseltem Fremdbereichs-bPK)

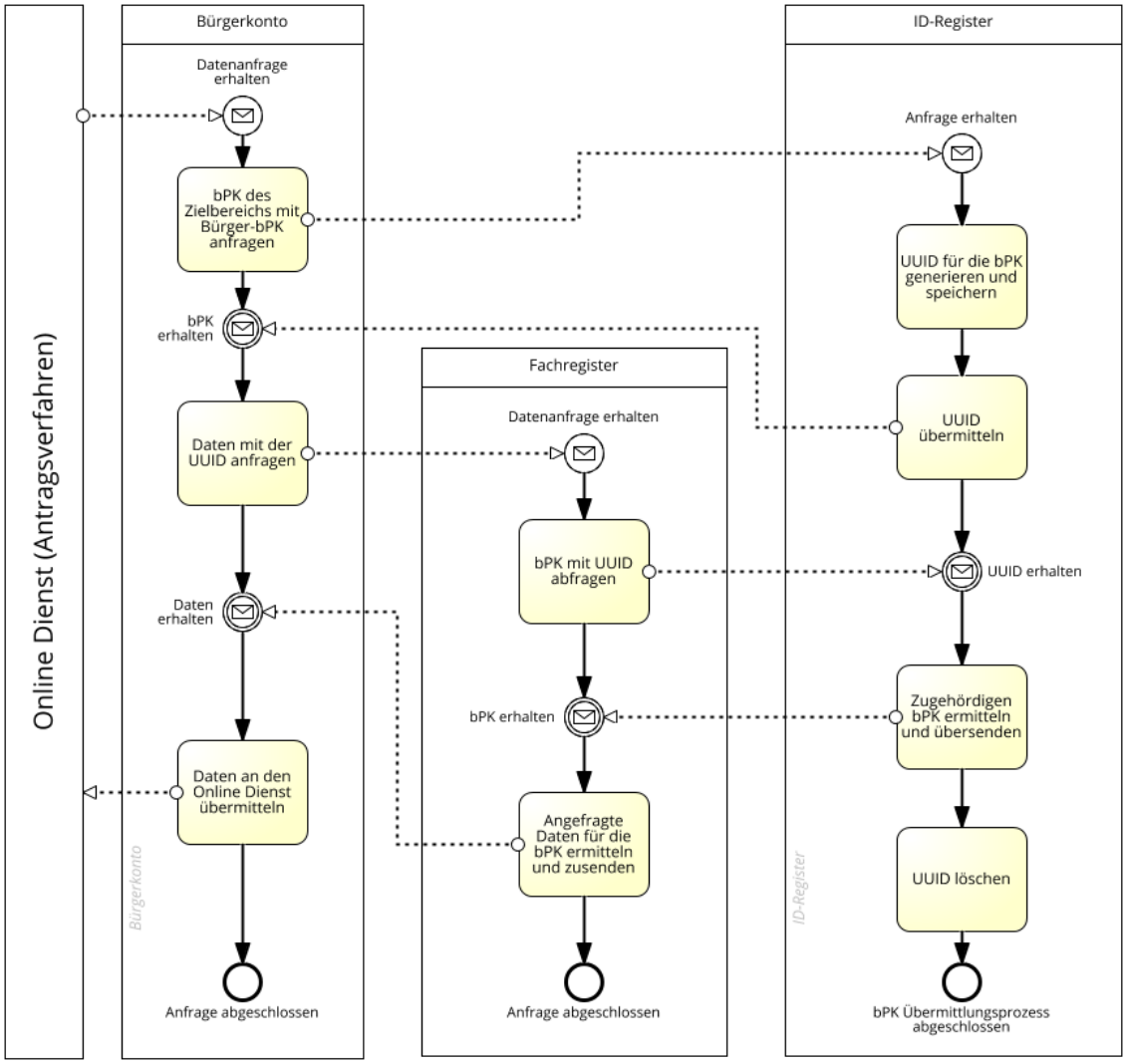


Abbildung 8 Datenaustauschszenario 2: Datenabruf während der Antragsstellung im Rahmen von Antragsverfahren nach OZG (Lösungsvariante 2 mit UUID)

4 Gemeinsame offene Klärungspunkte für das einheitliche Personenkennzeichen und die bereichsspezifischen Personenkennzeichen

4.1 Aufbau des ID-Registers als technisch separates System unter organisatorisch getrennter Verantwortung

Sowohl bei einer einheitlichen Kennziffer als auch bei bereichsspezifischen Kennziffern muss die Frage gelöst werden, wer das ID-Register führt und wie es technisch und organisatorisch mit dem Datenbestand des BZSt verbunden oder von diesem getrennt ist.

4.2 Vergabe von Kennziffern für nicht in Deutschland gemeldete Personen

Grundsätzlich besteht die Notwendigkeit, im Rahmen von elektronischen Verwaltungsverfahren auch die nicht in Deutschland gemeldeten Verwaltungskunden zu identifizieren und einen automatisierten Zugriff auf bestehende Datenbestände dieser Personen zu ermöglichen. Bislang sind im BZSt nur diejenigen erfasst, die in Deutschland einer Steuerpflicht unterliegen. Zukünftig müssen auch diejenigen erfasst werden, die im Ausland wohnen, aber in Deutschland einen Verwaltungskontakt – jenseits der Steuer – haben. Für diesen Personenkreis ist eine Lösung zu finden, unabhängig von der Frage, ob es eine einheitliche oder bereichsspezifische Kennziffer geben soll. (Hierfür hat Österreich bspw. ein Ergänzungsregister geschaffen, um solche Personengruppen zu erfassen)

Mit Hinblick auf das Single Digital Gateway und die rechtliche Verpflichtung, europaweite Registerzugriffe für alle EU-Bürger für SDG-Leistungen zu ermöglichen, wäre hiermit auch eine rechtliche Verpflichtung seitens der EU verbunden.

4.3 Fehlende Definition von Kernregistern und unklare Abgrenzung zu Fachverfahren

In der aktuellen Diskussion fehlt es an einer einheitlichen Definition von Kernregistern oder auch Registern im Allgemeinen. Oft werden diese Begriffe mit behördlichen Datenbeständen im Rahmen von Fachverfahren in synonymer Weise benutzt. Andere Länder wie Österreich mit ihrer Definition eines Registerkerns[4] oder auch Dänemark mit dem Danish Basic Data Program[5] haben schon seit 2010/2011 sehr früh einen klaren ressortübergreifenden konzeptionellen Rahmen gelegt, um darauf aufbauend Infrastrukturen und Optimierungsmaßnahmen für Register planen und umzusetzen. Etwas Vergleichbares fehlt bislang in Deutschland.

Diese begriffliche Unklarheit und faktisch fehlende staatliche Definition von Kernregistern in Deutschland führt dazu, dass viele Herausforderungen und fachliche Erfordernisse mit Hinblick auf einen Identifier für Datensätze und Datenaustauschverfahren und -infrastrukturen nicht klar identifiziert werden können.

Eine solche Klarheit ist unabhängig von einem Identifiermodell zwingend notwendig, um die fachlichen Anforderungen und die Rahmenbedingungen an die Registermodernisierung sowie die Infrastrukturen für Identifier zu definieren und zu bewerten. Erste Grundlagen für eine

[4] https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde.html
[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/25/Danish+Basic+Data+Program

solche Definition finden bspw. in der Erhebung des Statistischen Bundesamts im Gutachten des Normenkontrollrats[6].

4.4 Ausgestaltung der Datenaustauschverfahren und –infrastrukturen

Für die Festlegung der Datenaustauschverfahren und -infrastrukturen im Sinne von konkreten Architekturmustern, Protokollen und Querschnittssystemen ist eine klare Definition der Anforderungen aus den fachlichen Austauschszenarien und aus einer detaillierten Datenschutz-, Sicherheits- und Risikobetrachtungen zwingend erforderlich. In diese Betrachtung gehören auch Anforderungen aus relevanten Initiativen wie dem angedachten Datenschutz-Cockpit. Aus dem jeweiligen Identifiermodell können aber auch noch zusätzliche Anforderungen aufgrund von Datenschutz-, Sicherheits- und Risikoaspekten entstehen.

Die Festlegung der Datenaustauschverfahren und –infrastrukturen für eine deutschlandweite und ressortübergreifende Registermodernisierung ist eine vom Identifiermodell unabhängige und zusätzliche Aufgabe, die aber, basierend auf einer gesamthaften Betrachtung der Anforderungen und ressortübergreifenden Rahmenbedingungen, zwingend umzusetzen ist.

[6] https://www.normenkontrollrat.bund.de/resource/blob/300864/476024/04a6019c945895d3587136ff2ce46b73/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-staba-register-data.pdf

Abbildungsverzeichnis

Eckpunktepapier zum Einsatz eines verfahrensübergreifenden Identifiers - „4-Corner Modell“

Fassung vom 10.01.2020

Frank Steimke, KoSIT

1 Motivation und Begründung

2 Eigenschaften der Infrastruktur

2.1 Die sektorübergreifende Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

2.2 Die bei der sektorübergreifenden Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

2.4 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

2.5 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

2.6 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

2.7 Die Vertraulichkeit der Datenübermittlung muss mindestens auf der Strecke zwischen den Transporteuren sichergestellt sein

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

3 Konkretisierung für die Innenverwaltung

1 Motivation und Begründung

Verlässliche Angaben zur Identität der betroffenen Person sind die Grundlage aller personenbezogenen Verwaltungsleistungen. Die öffentliche Verwaltung speichert Daten zu Personen auf der Basis entsprechender Befugnisse in elektronisch geführten Registern, die nach dem Prinzip der behördlichen Zuständigkeit fachlich und häufig auch geografisch dezentral organisiert sind. Bei der elektronischen Abwicklung von Verwaltungsverfahren muss die eindeutige Zuordnung von Datensätzen in Registern zur jeweils betroffenen Person gewährleistet werden. Die irrtümliche Zuordnung von Datensätzen zur falschen Person muss ebenso ausgeschlossen werden, wie die ergebnislose Suche trotz vorhandener Datensätze.

Für eine verlässliche Zuordnung von Datensätzen in Registern zur betroffenen Person dürfen in Teilbereichen der öffentlichen Verwaltung eindeutige Identifikatoren genutzt werden. Beispiele hierfür sind die Steuer-ID (§ 139 AO) und die AZR Nummer (§ 3 AZRG). Ihre Verwendung ist jeweils nur für bestimmte Geschäftsvorfälle zulässig.

Verfahrensübergreifend wird derzeit häufig eine Kombination von Stamm- bzw. Basisdaten der betroffenen Person für eine Identifikation herangezogen (Name, Angaben zur Geburt, aktuelle Anschrift). Dieser faktisch vorhandene „sprechende Identifikator“ weist sowohl funktionale als auch datenschutzrechtliche Mängel auf.

Vor diesem Hintergrund hat die IMK die Einführung eines registerübergreifenden Identitätsmanagements beschlossen (210. Sitzung im Juni 2019, TOP 12). Es soll ein Identitätsregister eingerichtet werden, in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden. BMI schlägt vor, das Identitätsregister unter Nutzung der Steuer-ID-Datenbank des BZSt einzurichten. Eine eindeutige Zuordnung der Personalienidentität über alle Register der öffentlichen Verwaltung hinweg soll mithilfe eines Identifiers sichergestellt werden. BMI schlägt vor, hierfür die Steuer-ID oder einen davon abgeleiteten Identifikator zu verwenden. Dieser Identifier ist eine Kennziffer im Sinne des Artikel 87 DSGVO.

Im Zuge der Einführung eines Identifiers müssen aus verfassungsrechtlichen Gründen Maßnahmen ergriffen werden die verhindern, dass es durch eine unzulässige Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von umfassenden Persönlichkeitsprofilen kommen kann. Zugleich muss sichergestellt sein, dass rechtmäßige Datenübermittlungen uneingeschränkt möglich sind und zuverlässig funktionieren. Für jede Datenübermittlung bedarf es zunächst einer entsprechenden Rechtsgrundlage. In der nach dem Prinzip der behördlichen Zuständigkeit dezentral organisierten Registerlandschaft der öffentlichen Verwaltung ist die *Zusammenführung* von Daten gleichbedeutend mit der *Übermittlung* von Daten. Daher soll die unzulässige Zusammenführung einzelner Lebens- und Personaldaten, die zur Erstellung von Persönlichkeitsprofilen führen könnte, dadurch ausgeschlossen werden, dass Kontrolle über Datenübermittlungen zwischen Behörden ausgeübt wird.

Zu diesem Zweck sollen innerhalb der Behörden- bzw. Registerlandschaft der öffentlichen Verwaltung *Sektoren* anhand fachlicher Kriterien definiert werden, beispielsweise *Finanzen / Gesundheit / Arbeit und Soziales / Innenverwaltung*. Sektor-übergreifenden Datenübermittlungen, die den Identifier enthalten, dürfen nur über eine technische Infrastruktur erfolgen, die die erforderlichen Kontrollmöglichkeiten des Staates gewährleistet.

Auf diese Weise wird mittels rechtlicher und technischer Maßnahmen sichergestellt, dass Datenübermittlungen zwischen Sektoren stets nur in einem kontrollierten und überwachten Umfeld stattfinden können. Die unkontrollierte Zusammenführung von Daten aus unterschiedlichen Sektoren ist nicht möglich, so dass die Erstellung von Persönlichkeitsprofilen durch „den Staat“ bzw. eine Behörde wirksam verhindert wird.

2 Eigenschaften der Infrastruktur

Nachfolgend werden Eigenschaften einer Infrastruktur für Datenübermittlungen zwischen Behörden genannt, die erforderlich sind, um die notwendigen Kontrollfunktionen bei Datenübermittlungen zwischen Sektoren ausüben zu können.

Die Eigenschaften werden abstrakt und technikneutral beschrieben. Zur Erläuterung der Eigenschaften wird die konkrete Umsetzung in der Innenverwaltung herangezogen. Die dabei genannten, konkreten Standards bzw. Komponenten dienen nur der Illustration.

Sektor-übergreifende Datenübermittlungen zwischen Behörden, die den Identifier enthalten, sind nur zulässig, wenn sie über eine technische Infrastruktur mit den nachfolgend genannten Eigenschaften erfolgt:

2.1 Die Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

*Die beiden Stellen, zwischen denen auf der Basis bestehender Rechtsgrundlagen übermittelt werden, werden als **Autor** bzw. **Leser** bezeichnet. Die Daten dürfen nicht direkt zwischen diesen beiden Stellen ausgetauscht werden, sondern es müssen Dritte Stellen beteiligt sein, bei denen die nachfolgend dargestellten Kontrollfunktionen wahrgenommen werden können.*

In der Innenverwaltung ist dieses Prinzip durch den Im Auftrag des IT-Planungsrats von der KoSIT herausgegebene OSCI Transport Standard und die vom IT-Planungsrat bereitgestellte Anwendung „Governikus“ realisiert. Für die Herstellung einer Verbindung (Vermittlungsdienst) wird das vom Bund und den Ländern gemeinsam betriebene „Deutsche Verwaltungsdiensteverzeichnis DVDV 2“ genutzt. Die Infrastruktur der Innenverwaltung wird gebildet durch die abgestimmte Nutzung technischer Standards und geeigneter, von der öffentlichen Verwaltung betriebener Anwendungen.

Die rechtliche Verpflichtung zur Anwendung dieser Infrastruktur ist u. a. in §§ 2, 3 der 1. BMeldDÜV für die Übermittlung von Meldedaten festgelegt.

2.2 Die bei der Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

Der Betreiber des Vermittlungsdienstes und die für den Transport zuständigen Stellen müssen selbst der staatlichen Kontrolle unterliegen.

In der Innenverwaltung ist diese Bedingung nach unserem Kenntnisstand für alle Betreiber der OSCI-Intermediäre (Anwendung Governikus des IT-Planungsrats) und alle als Clearing- bzw. Vermittlungsstellen agierenden Organisationseinheiten ebenso gewährleistet, wie für alle Betreiber des Deutschen Verwaltungsdiensteverzeichnisses DVDV auf Bundes- und Landesebene.

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

*Es muss mindestens protokolliert werden: **Wer** übermittelt Daten **an Wen** aus welchem **Anlass** zu welchem **Zeitpunkt**.*

In der Innenverwaltung führen die am Transport beteiligten Stellen entsprechende Protokolle auf Basis des OSCI Laufzettels. Die konkreten Inhalte der Protokollangaben und die Aufbewahrungsfristen sind innerhalb der Innenverwaltung abgestimmt.

In der Innenverwaltung nehmen die Betreiber der OSCI Intermediäre eine zusätzliche, ursprünglich nicht vorgesehene Kontrollfunktion wahr: nach dem Erhalt einer Nachricht prüfen sie im Zusammenspiel mit dem Vermittlungsdienst DVDV, ob die Behördenkategorie des Absenders und der Anlass der Datenübermittlung zusammenpassen. Beispiel: wenn eine Nachricht aus Anlass einer Fortschreibung von Meldedaten gemäß § 23 BMG übermittelt wird, dann muss der Absender der Nachricht eine Behörde der Kategorie „Meldebehörde" sein. Andernfalls wird ein Fehler gemeldet, auf den entsprechend reagiert werden kann.

2.4 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

Sowohl die originären Aufgaben des sicheren Transports bzw. der Herstellung (Vermittlung) einer Verbindung, als auch die hier beschriebenen Kontroll- und Überwachungsfunktionen müssen die Dritten Stellen auch dann in vollem Umfang wahrnehmen können, wenn sie keine Kenntnis vom eigentlichen Nachrichteninhalt haben.

*Eine andere Formulierung dieser Eigenschaft lautet: Die Infrastruktur muss die Möglichkeit einer **Ende-zu-Ende Verschlüsselung** zwischen den beiden behördlichen Kommunikationspartnern (Autor und Leser) unterstützen.*

In der Innenverwaltung wird dieses Prinzip zunächst durch die Verwendung des OSCI Transport Standards realisiert. Dieser unterstützt die kryptografisch unterschiedliche Behandlung der Metadaten und der eigentlichen Inhaltsdaten, so dass der sichere Transport auch dann gewährleistet wird, wenn die Betreiber der OSCI Intermediäre keinerlei Kenntnis vom Nachrichteninhalt erlangen können.

Angesichts wachsender Anforderungen an die Infrastrukturen der öffentlichen Verwaltung wird dieses Prinzip durch den ebenfalls im Auftrag des IT-Planungsrats von der KoSIT herausgegebenen Standard XTA erweitert, und noch stärker auf die Anforderungen der als Transporteur agierenden Stellen angepasst.

2.5 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

*Die Identität der behördlichen Kommunikationspartner (**Autor** und **Leser**) soll durch Zertifikate nachgewiesen werden, die einer von der öffentlichen Verwaltung kontrollierten Publik Key Infrastructure (PKI) entstammen.*

2.6 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

Durch diese Festlegung soll ausgeschlossen werden, dass Transporteure eine personenbezogene Profilbildung betreiben können, die über alle innerbehördlichen Datenübermittlungen zu einer bestimmten Person Auskunft geben könnte

2.7 Die Vertraulichkeit der Datenübermittlung wird mindestens auf der Strecke zwischen den Transporteuren durch eine hinreichende Verschlüsselung sichergestellt.

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

Diese Dritte Stelle wird Vermittlungsdienst oder Verzeichnisdienst genannt. Sie versorgt die Transporteure mit den für den Transport erforderlichen Angaben (z. B. öffentlichen

Schlüsseln des Empfängers zwecks Gewährleistung der Vertraulichkeit durch Verschlüsselung).

Die Herstellung einer Verbindung ist nur dann möglich, wenn es für den angegebenen Zweck und die angegebenen Kommunikationspartner einen entsprechenden Eintrag im Vermittlungs- bzw. Verzeichnisdienst gibt. Anders ausgedrückt: Datenübermittlungen, für die keine Rechtsgrundlage angegeben werden kann, oder bei denen die Angaben zu Sender, Empfänger und Zweck nicht zueinander passen, können nicht vermittelt werden.

In der Innenverwaltung kommt für diese Zwecke das DVDV 2 zum Einsatz.

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

Die Tatsache, dass nur solche Datenübermittlungen vermittelt werden können, für die es einen hinsichtlich der Kommunikationspartner und dem Zweck passenden Eintrag gibt, ist für die Kontrollfunktionen entscheidend. Daher dürfen Eintragungen nur in einem kontrollierten Verfahren vorgenommen werden.

Nur die durch den Bund bzw. die Länder bestimmten „pflegenden Stellen" sind befugt, Einträge in das DVDV 2 vorzunehmen, welches in der Innenverwaltung als Vermittlungsdienst agiert. Dafür erforderliche Datenübermittlungen zwischen „pflegenden Stellen" und dem DVDV 2 sind ebenfalls durch OSCI-Transport gesichert. Dadurch werden unbefugte Manipulationen verhindert, gleichzeitig wird Nachvollziehbarkeit sichergestellt.

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

Entsprechend der bisherigen Ausführungen gehören zur Infrastruktur folgende Anwendungen und Interoperabilitätsstandards:

- *Der Vermittlungs- bzw. Verzeichnisdienst. In der Innenverwaltung: DVDV 2*
- *Der oder die Transporteure. In der Innenverwaltung: die Betreiber der OSCI Intermediäre.*
- *Eine Public Key Infrastrukture (PKI) für den Nachweis der Identität der Kommunikationspartner*
- *Ein oder mehrere Standards für die Interoperabilität zwischen allen an der Datenübermittlung beteiligten Stellen der Infrastruktur. Diese müssen als offene Standards im Sinne der Free Software Foundation Europe e.V. (FSFE) betrieben werden.*

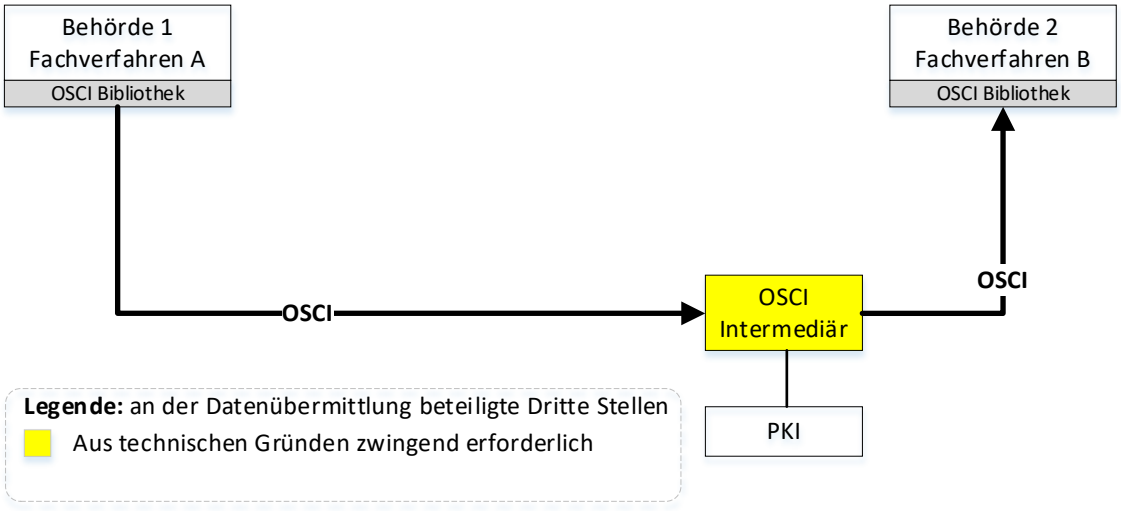
  In der Innenverwaltung sind dies die beiden im Auftrag des IT-Planungsrats herausgegebenen Standards OSCI-Transport und XTA.

Durch die Verpflichtung zur (Weiter-) Entwicklung aller zur Infrastruktur gehörenden Komponenten (Anwendungen und Standards) wird die notwendige Transparenz gewährleistet, die wiederum den Aufsichtsbehörden die Wahrnehmung ihrer Kontrollaufgaben ermöglicht.

3 Konkretisierung für die Innenverwaltung

Nachfolgend werden die allgemein gehaltenen, technikneutralen Anforderungen des Abschnitt 2 für die in der Innenverwaltung vorhandene Infrastruktur konkretisiert und erläutert. Sie basiert auf Standard OSCI Transport. Er wurde durch die OSCI-Leitstelle (Vorläufer der KoSIT) gemeinsam mit dem BSI entwickelt und im Jahr 2002 erstmalig veröffentlicht. Er ist fachunabhängig, das heißt, für die Datenübermittlung zwischen beliebigen Kommunikationspartnern innerhalb und außerhalb der öffentlichen Verwaltung geeignet. Er erfordert zwingend eine Infrastrukturkomponente, bei der kryptografische Funktionen gebündelt und Nachrichten aufbewahrt werden können (Intermediär). Betreiber der Intermediäre können ihre Aufgaben ohne Kenntnis der Inhaltsdaten wahrnehmen (Ende-zu-Ende Verschlüsselung). Dies ermöglicht den Betrieb von Intermediären durch zentrale Stellen. Das ursprüngliche Konzept (ca. 2005) ist in Abbildung 1 dargestellt.

Abbildung 1: Ursprüngliches Konzept für OSCI



Dieses Konzept erwies sich jedoch als nicht ausreichend, weil die Komplexität der Organisation der sicheren Datenübermittlung mit tausenden von Kommunikationspartnern auf der Ebene des Bundes, der Länder und vor allem aller Kommunen unterschätzt worden ist.

Die inzwischen tatsächlich vorhandene, in der Praxis bewährte Infrastruktur der Innenverwaltung ist dementsprechend komplexer. Sie ist Abbildung 4 in dargestellt. Sie wird in identischer bzw. sehr ähnlicher Form auch im Bereich der Übermittlung elektronischer Gewerbeanzeigen gemäß § 14 Absatz 8 GewO und im elektronischen Rechtsverkehr genutzt.

Verzeichnisdienst DVDV 2

Bei einer Vielzahl von Kommunikationspartnern ist eine zentrale Stelle erforderlich, die eine Übersicht über alle insgesamt angebotenen elektronischen Dienste führt. Hierfür wurde das Deutsche Verwaltungsdiensteverzeichnis DVDV eingeführt. Darin ist beispielsweise verzeichnet, welche technischen Kommunikationsparametern für die Behörde erforderlich sind, die den Dienst der Abruf von Meldedaten gemäß § 38 BMG für die Kommune Bremerhaven anbietet.

Nähere Informationen zum DVDV 2 und den aktuell eingetragenen Diensten sind auf der Webseite des ITZ Bund erhältlich [1, 2].

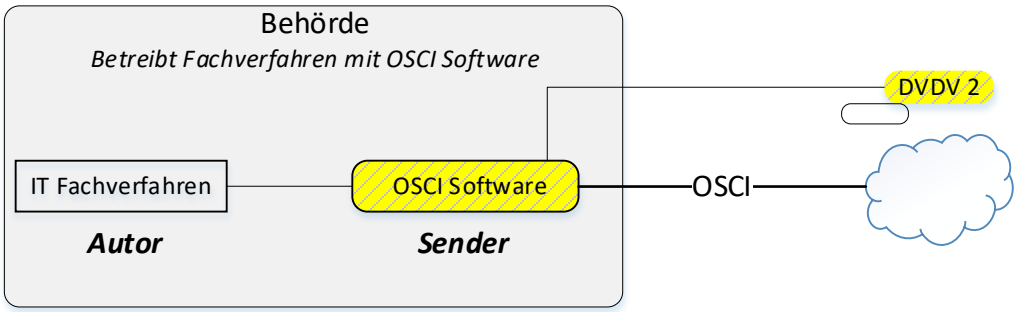
Organisation des sicheren Transports als eigenständige Aufgabe

Bei einer Vielzahl von Kommunikationsbeziehungen ist die Organisation des Nachrichtentransports eine komplexe Aufgabe. Sie beinhaltet den Umgang mit elektronischen Zertifikaten, die Identifikation und Behebung technischer Fehler, die Protokollierung etc.

Transportaufgaben wurden daher ausgelagert und eigenen Rollen zugewiesen. Diese werden als **Sender** bzw. **Empfänger** und zusammenfassend als **Transporteure** bezeichnet. Es gibt unterschiedliche Ausprägungen, die in Abbildung 2 und Abbildung 3 jeweils für die Rolle Sender dargestellt werden.

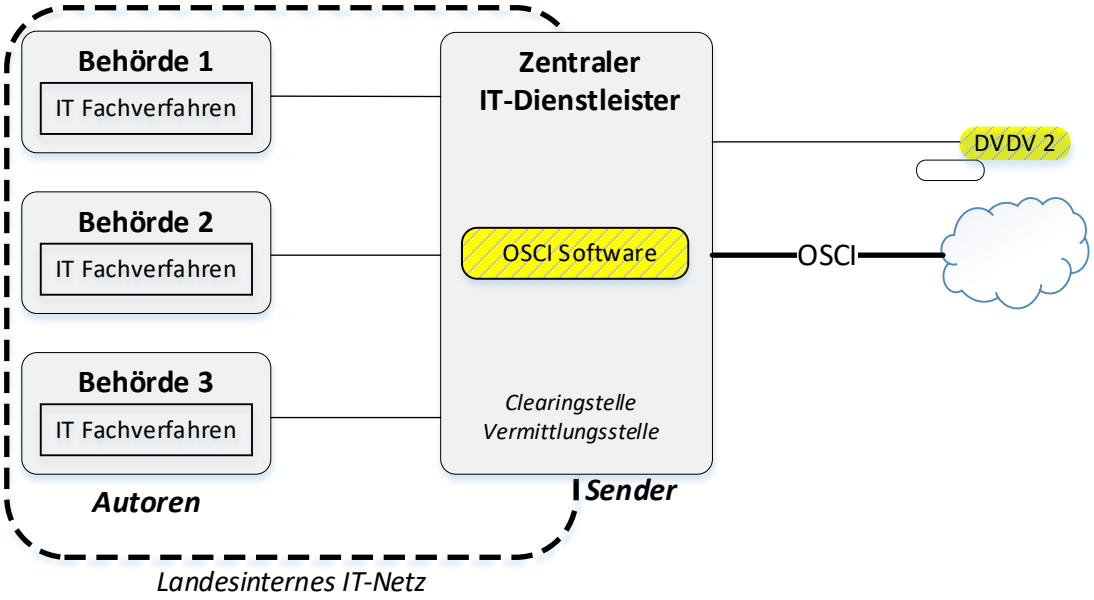
Es kann sich um eine spezielle Software handeln, die als Ergänzung eines IT-Fachverfahrens bereitgestellt wird, um die Datenübermittlung mit OSCI zu organisieren (teilweise als Kommunikationsserver bezeichnet). In diesem Fall agiert die Behörde, bei der das Fachverfahren betrieben wird, gleichzeitig als Transporteur (siehe Abbildung 2).

Abbildung 2: Anbindung mit OSCI Software (Kommunikationsserver)



Häufiger ist jedoch die Errichtung einer für ein Bundesland zentralen Clearing- oder Vermittlungsstelle (siehe § 2 Abs. 3 der 1. BMeldDÜV), bei der die Rolle des Transporteurs im Wege der Datenverarbeitung im Auftrag der angeschlossenen Fachbehörden wahrgenommen wird.

Abbildung 3: Clearing- bzw. Vermittlungsstellen



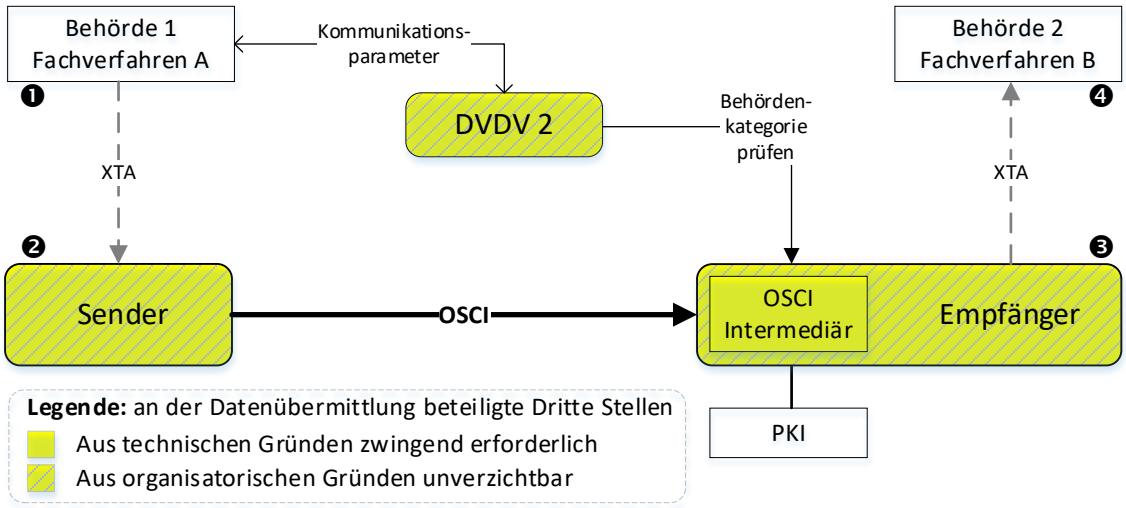
Die Betreiber der für die OSCI Infrastruktur zuständigen Clearingstellen haben sich selbstorganisiert zusammengeschlossen und tagen regelmäßig.

Unabhängig von der Art der Anbindung ergibt sich aufgrund der konzeptionellen Trennung der Aufgaben einer Fachbehörde, die als Autor bzw. Leser einer Fachnachricht agiert, und der

Organisation des sicheren Transport die in Abbildung 4 schematisch dargestellte Infrastruktur der Innenverwaltung. Sie ist seit 2007 ohne nennenswerte Störungen in Betrieb. Jährlich werden mehrere 100 Millionen Nachrichten übermittelt.

Solche Infrastrukturen werden als *4-Corner Modell* bezeichnet (die vier Ecken sind in Abbildung 4 gekennzeichnet). Nach unserem Kenntnisstand ist die Tatsache, dass die beim Transport zu beteiligenden Dritten Stellen ihre Aufgabe auch ohne Kenntnis des Nachrichteninhalts erbringen können, zumindest nicht selbstverständlich (ggfs. ein Alleinstellungsmerkmal).

Abbildung 4: Infrastruktur der Innenverwaltung (schematisch)



Dritte Stellen im Sinne des Eckpunktepapiers

Hinsichtlich der Aussagen des Eckpunktepapiers bedeutet das insbesondere, dass die als Transporteure agierenden Stellen (*„Sender“* und *„Empfänger“* in Abbildung 4 nicht aus technischen Gründen zwangsläufig mit dem Einsatz von OSCI verbunden sind. Dies wäre lediglich der OSCI Intermediär. In der Praxis ist aber deutlich geworden, dass die Organisation des sicheren Nachrichtenversands in einer flächendeckenden Infrastruktur der öffentlichen Verwaltung so komplex ist, dass er spezialisierten Rollen übertragen werden muss.

Dies sind meistens rechtlich eigenständige Organisationseinheiten, deren originäre Aufgabe darin besteht, im Auftrag angeschlossener IT-Fachverfahren die effiziente und verlässliche Datenübermittlung gemäß einschlägigen Rechtsgrundlagen sicherzustellen. Sofern ihnen im Rahmen der Einführung eines verfahrensübergreifenden Identifiers zusätzliche Kontrollaufgaben bei Sektor-übergreifenden Datenübermittlungen zugewiesen werden, sollte ggfs. ihre rechtliche Einordnung neu bestimmt werden.

Neben den Transporteuren kommt auch der Verzeichnisdienst DVDV 2 als *Dritte Stelle* zur Wahrnehmung von Kontrollfunktionen im Sinne des Eckpunktepapiers in Betracht.

Welche Lösung am besten geeignet ist, wird noch zu bestimmen sein, wenn

a) Klarheit über die „Sektoren“ hergestellt worden ist, an deren Grenzen Kontrollfunktionen eine Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen verhindern; und
b) Die dort erforderlichen Kontrollfunktionen näher bestimmt worden sind.

Weblinks

[1] DVDV bei ITZ Bund

[2] Übersicht der Dienste im DVDV