Schweizerische Informatikkonferenz
Conférence suisse sur l'informatique
Conferenza svizzera sull'informatica
Conferenza svizra d'informatica

Gutachten

AHV-Nummer als einheitlicher, organisationsübergreifender Personenidentifikator

Version 2.0, 03.10.2015

Dieses Gutachten wurde erstellt von der

Berner
Fachhochschule BFH
E-Government-Institut

Autorenschaft: Brian Olivier, BFH
Brugger Jérôme, BFH
Dungga Angelina, BFH
Hefti Esther, Kt. ZH
Selzam Thomas, BFH
Spichiger Andreas, BFH
Weissenfeld Katinka, BFH

Inhaltsverzeichnis

1 Management Summary

Dieses Gutachten wurde im Auftrag der Schweizerischen Informatikkonferenz (SIK) erstellt. Die Ziele des Gutachtens sind:

- die Risiken und Kosten einer Nichtverwendung der AHVN13 als einheitlicher, organisationsübergreifender Personenidentifikator anhand von Fallbeispielen zu veranschaulichen; und
- die Regelungen im Ausland zu ermitteln, welche die gute Verwendung eines nationalen, eindeutigen Personenidentifikators erlauben.

Es wurden Interviews mit IT-, Geschäfts- oder Bereichsverantwortlichen in der öffentlichen schweizerischen Verwaltung und mit Bereichsverantwortlichen der dänischen, niederländischen und spanischen Staatsverwaltung geführt. Zusätzlich stellte sich der Vorsitzende eines unabhängigen Expertenrates in Dänemark für ein Interview zur Verfügung, der sich für den Datenschutz und die Datensicherheit in der digitalen dänischen Gesellschaft einsetzt.

Das Gutachten beschreibt in einem ersten Teil die heutige Verwendung der AHVN13 in der Schweiz und insbesondere die mit der Nichtverwendung der AHVN13 einhergehenden Risiken sowie die Regelungen im Ausland. Der zweite Teil enthält einen Systemvergleich, eine Gesamtbetrachtung der Risiken, eine Analyse der Implikationen für den Datenschutz sowie eine ansatzmässige Kostenbetrachtung.

Die Ergebnisse bestätigen die Vermutung, dass das Fehlen eines eindeutigen Personenidentifikators zu Risikosituationen führen kann. Besonders erstaunlich ist der Befund, dass mangels Eindeutigkeit bei der Identifikation von Personen in Verwaltungsabläufen u.a. Datenschutzverletzungen die Folge sind. Die Erfahrungen aus dem Ausland zeigen, dass die Verwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators mit dem Datenschutz vereinbar und auch in der praktischen Umsetzung nicht problematisch ist. Die Überlegungen zu alternativen Lösungen zeigen, dass die heutige Situation sehr grosse Mehrkosten verursacht. Die Erfahrungen aus dem Ausland bestätigen eine höhere Effektivität und Effizienz mit einem einheitlichen Personenidentifikator. Zudem wurde festgestellt, dass die Schweiz bereits über die nötige Infrastruktur für den Betrieb eines solchen Identifikators verfügt.

Es empfiehlt sich, die Identifikationsprobleme, die in zahlreichen Verwaltungsabläufen vorkommen, ganzheitlich zu lösen und nicht jedes einzeln je im betreffenden Fachbereich. Die Einführung der AHVN13 als einheitlicher, organisationsübergreifender Personenidentifikator wird, aufgrund fehlender echter Alternativen dringend empfohlen.

2 Einleitung

In der Schweiz gibt es keinen einheitlichen, organisationsübergreifend genutzten Personenidentifikator. Die Nutzung des verbreitetsten Identifikators AHVN13 erfordert eine gesetzliche Grundlage für jeden Nutzenden. Daraus ergeben sich operative Herausforderungen und Gefahren durch mangelnde Eindeutigkeit bei der organisationsübergreifenden Datenverarbeitung. Die Einführung einheitlicher, organisationsübergreifender Personenidentifikatoren wurde bis dato durch Datenschutzbedenken verhindert.

Im Auftrag der Schweizerischen Informatikkonferenz (SIK) erstellt die Berner Fachhochschule (BFH) ein Gutachten mit dem Ziel, anhand von allgemeinverständlichen Beispielen die Gefahren und Risiken aufzuzeigen, welche sich aus der Nichtverwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators ergeben. Ferner stellt sie die Situation und insbesondere die Regelungen in anderen Ländern, in welchen ein einheitlicher, organisationübergreifender Identifikator verwendet wird, kurz dar.

Gegenstand der Betrachtung sind Fälle innerhalb der öffentlichen Verwaltung, in denen ein eindeutiger Personenidentifikator verwendet oder nachgefragt wird. Beschrieben werden indessen ausschliesslich Fallbeispiele, in denen ein Informationsaustausch zwischen Behörden aufgrund eines gesetzlichen Auftrags erforderlich und aufgrund ausreichender gesetzlicher Grundlagen zulässig ist.

Dieses Dokument legt zuerst die aktuelle Situation in der Schweiz in Bezug auf die Verwendung der AHVN13 als eindeutiger Personenidentifikator dar. Warum und in welchen Fällen die eindeutige Identifizierung von Personen in Verwaltungsabläufen notwendig ist, wird in Kapitel 4 anhand von Fallbeispielen aufgezeigt. Konkret wird die Situation bei der Mehrwertsteuerunterstellung von Einzelfirmen, im Grundbuch, im Verkehrsbereich und im Strafregister beschrieben. Dabei handelt es sich um eine kleine Auswahl einer grossen Zahl ähnlich gelagerter Prozesse. Auch die in den einzelnen Fällen gewählten Lösungsstrategien werden hier diskutiert. Kapitel 5 geht auf die Regulierungen im vergleichbaren Ausland ein, die in Zusammenhang mit einem nationalen einheitlichen und organisationsübergreifenden Personenidentifikator getroffen wurden. Im Anschluss daran werden in Kapitel 6 die Ergebnisse aus der Risiko-, Kosten- und Datenschutzperspektive diskutiert, sowie die Situation in der Schweiz mit der Situation im Ausland verglichen. Abschliessend werden unter Berücksichtigung der ausgewählten Fallbeispiele aus der Schweiz und den Erfahrungen mit dem nationalen Personenidentifikator aus Dänemark, den Niederlanden und Spanien eine Schlussfolgerung und eine Empfehlung abgegeben.

Im Sinne des Auftrages wird besonders auf eine leicht verständliche und für jede Leserin und jeden Leser zugängliche Sprache Wert gelegt. Ziel ist es, die Situation auf anschauliche Art und Weise darzustellen.

3 Aktuelle Situation

3.1 Einleitung

In der Schweiz wurde 2008 die neue AHV-Nummer AHVN13 eingeführt. Sie ersetzt die alte 11-stellige AHV-Nummer und wurde ursprünglich für die Verwendung im Sozialversicherungsbereich der 1. Säule konzipiert.

Sie ist die einzige Nummer, welche die gesamte Wohnbevölkerung in der Schweiz durch die Vergabe einer eindeutigen, nicht-sprechenden Nummer erfasst. Um die laufende Zuordnung und die Eindeutigkeit der Nummer zu gewährleisten, hat die Zentrale Ausgleichsstelle (ZAS) eine Infrastruktur und dazugehörige Prozesse zur Vergabe und Verwendung der Nummer implementiert. Der Betrieb dieser Infrastruktur kostet die Steuerzahlenden und die AHV/IV-Beitragspflichtigen jährlich ca. 5

Millionen Schweizer Franken[1]. Dessen Einführung verursachte ausserhalb der AHV-IV Kosten von ca. 20 Millionen Schweizer Franken[2].

Dieses Kapitel legt die heutige Situation in Zusammenhang mit der Verwendung der AHVN13 als eindeutiger Personenidentifikator in der Schweiz dar.

3.2 Die AHVN13

In zahlreichen Verwaltungsabläufen besteht ein zwingender Bedarf nach einem eindeutigen Personenidentifikator, der organisationsübergreifend eingesetzt werden kann. Die am 1. Juli 2008 offiziell eingeführte AHV-Nummer AHVN13 bietet sich aus folgenden Gründen als Personenidentifikator an [1]:

- Sie wird allen in der Schweiz wohnhaften Personen zugeteilt[3];
- Die Eindeutigkeit der Nummer wird mittels permanentem Qualitätsmanagement der Datenbank soweit als möglich gewährleistet;
- Die Zuteilung der Nummer erfolgt so früh wie möglich nach der Geburt oder nach Zuzug in die Schweiz;
- Sie basiert nicht auf persönlichen Identifikationsmerkmalen einer Person und lässt somit keine Rückschlüsse auf den Nummerninhabenden zu (d.h. sie ist nicht sprechend);
- Sie wird in der Regel nur einmal zugeteilt und bleibt auch nach dem Tod des Nummerinhabenden gültig.

3.3 Die UPI-Datenbank

Die Zuordnung und Verwaltung der AHVN13 ist Aufgabe der ZAS [2]. Für die Erfüllung dieser Aufgabe hält sie das Monopol und betreibt die UPI-Datenbank. Die für die Zuteilung und Pflege notwendigen Informationen erhält UPI hauptsächlich vom Eidgenössischen Zivilstandsregister (Infostar) und vom Ausländer- und Asylbewerberregister (ZEMIS) [3].

Die in der UPI-Datenbank geführten Daten können in folgende Sammelbegriffe zusammengefasst werden:

- Offizieller Familienname;
- Ledigenname;
- Offizielle(r) Vorname(n);
- Geschlecht;
- Geburtsdatum;
- Geburtsort;
- Staatsangehörigkeit;
- Familiennamen und Vornamen der Eltern [4].

Die genaue Benennung der Merkmale und deren Ausprägungen sind im amtlichen Katalog der Merkmale des Bundesamtes für Statistik BFS [5] beschrieben.

3.4 Die Verwendung der AHVN13

Die gesetzliche Grundlage für die Verwendung der AHVN13 im Sozialversicherungsbereich liegt in den umfassenden Regelungen des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG). Dort ist ebenfalls festgehalten, dass jede systematische Verwendung der AHVN13 ausserhalb der Sozialversicherung einer gesetzlichen Grundlage auf Stufe Bund oder Kanton (AHVG Art. 50e) bedarf und der ZAS gemeldet werden muss.

[1] Quelle: ZAS (EFD)

[2] Quelle: ZAS (EFD) / BFS (EDI)

[3] Liegt eine Notwendigkeit vor, erlaubt das System auf Anfrage die Zuteilung einer Nummer auch an nicht in der Schweiz wohnhaften Personen.

Bereits heute nutzen eine Vielzahl von Behörden sämtlicher föderalen Ebenen sowie Krankenkassen und Pensionskassen (2. Säule) die Dienstleistungen des UPI und verwenden die AHVN13 als eindeutigen Personenidentifikator in ihren Fachapplikationen. Das Verzeichnis der systematischen Benutzerinnen und Benutzer der AHVN13 der ZAS zählt zum heutigen Stand ca. 12‘760 systematische Benutzer [6]. Diese Liste umfasst sowohl die einzelnen AHV-Durchführungsorgane als auch Institutionen, die im Rahmen des AHV-Gesetzes oder des Gesetzes zur Registerharmonisierung zur Benutzung der AHVN13 berechtigt sind. Ausserhalb der AHV-Institutionen sind die Einwohnerregister, das Bundesamt für Statistik (BFS), der Fiskalbereich, die BVG-Einrichtungen sowie die Armee zur Verwendung der AHVN13 berechtigt. Weiter ist es Krankenkassen, aufgrund der Verordnung über die neue Versichertenkarte [7] und den mit der Sozialhilfe betrauten Stellen (Art. 50e AHVG) erlaubt, die AHVN13 zu nutzen. Der Grossteil der in der Liste der Benutzerinnen und Benutzer vorkommenden Institutionen ist dem Ausbildungsbereich zuzuordnen.

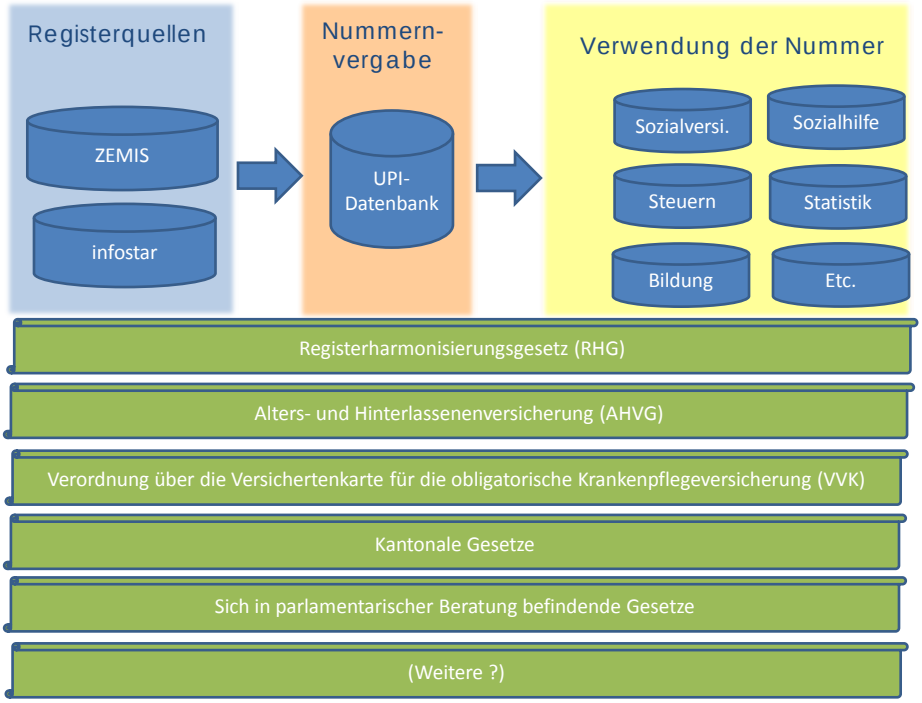

Abbildung 1: Modellhafte Darstellung des heutigen Systems rund um die AHVN13 (Quelle: Eigene Darstellung)

In Abbildung 1 wird das heutige System rund um die AHVN13 vereinfacht bildlich dargestellt. Die UPI-Datenbank erscheint als zentrales Element, das Personendaten erhält, die Nummernzuordnung vornimmt und die Daten an gesetzlich berechtige Benutzende zur Verfügung stellt. Als Hauptquellen sind die Register ZEMIS und infostar dargestellt[4].

Die grün gefärbten Elemente zeigen die gesetzlichen Grundlagen, die im System integriert sind. Regelungen, die die Registerführung betreffen, sind im AHVG und im Registerharmonisierungsgesetz (RHG) festgehalten. Bestimmungen zur Nutzung der Nummer sind in einer Vielzahl von Gesetzen geregelt. Es sind nicht alle Nutzungsberechtigten und deren dazugehörigen Gesetze illustriert. Für die Berechtigung der Nutzung wird teilweise auf andere Gesetzestexte verwiesen.

3.5 Datenschutz

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) verfolgt die Diskussion um die Verwendung der AHVN13 bereits seit ihrer Einführung. Er sieht Gefahren für den Datenschutz

[4] Zur Komplexitätsreduktion verzichtet die Darstellung auf die vollständige Nennung sämtlicher beteiligten Register und stellt nur die beiden Hauptquellregister dar.

durch die Verwendung der AHVN13. Insbesondere bereitet die missbräuchliche, zweckwidrige Verknüpfung von Personendaten dem EDÖB Sorgen.

Die Gefahren, die in Zusammenhang mit einem einheitlichen, organisationsübergreifenden Personenidentifikator auftreten, wurden in einem von Prof. Dr. iur. Giovanni Biaggini (2002) erstellten Rechtsgutachten [8] besprochen. Das Gutachten sieht eine besonders hohe Gefahr beim Einsatz eines einheitlichen, organisationsübergreifenden Personenidentifikators in Zusammenhang mit Daten zur elektronischen Stimmabgabe, Gesundheitsdaten und Daten über strafrechtliche Verfolgungen und Sanktionen. Des Weiteren wird die Angst beschrieben, dass Personendaten ohne Kenntnis der betreffenden Personen in Datensammlungen erhoben werden und dadurch die Souveränität über die eigenen Daten verloren geht.

Das Gutachten weist darauf hin, dass die Einführung und Verwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators durch ein überwiegendes öffentliches Interesse gerechtfertigt und verhältnismässig sein und den einschlägigen verfassungsrechtlichen Anforderungen genügen müsse. Ob das öffentliche Interesse in diesem Fall eine Lockerung der Zweckbindung legitimiert und diese verhältnismassig ist, wurde im Rahmen des Gutachtens nicht abschliessend beurteilt. Ist das Kriterium des öffentlichen Interesses jeweils kontextbezogen abzuwägen, so verlangt das Kriterium der Verhältnismässigkeit einen Erforderlichkeitsnachweis. Konkret gilt es abzuschätzen, ob gangbare Alternativen existieren [8].

Aus Sicht des EDÖB wird die missbräuchliche Verwendung von personenbezogenen Daten durch den Einsatz eines bereichsübergreifenden Personenidentifikators technisch erleichtert. Der Gefahr von unrechtmässigen Datenverknüpfungen soll durch die Nichtverwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators begegnet werden [9]. Diese Haltung hat sich seit der Einführung der AHVN13 nicht geändert, wie einer Medienmitteilung vom 16.04.2014 des EDÖB zu entnehmen ist [10].

3.6 Bestrebungen zur systematischen Nutzung der AHVN13

Zurzeit liegen im Parlament drei Botschaften[5] vor, die die systematische Verwendung der AHVN13 einfordern.

Sobald eine Behörde personenbezogene Daten mit einer anderen Behörde austauschen oder behördenintern mit einem anderen IT-System verbinden muss, muss sie sich entscheiden, ob

1. sie die Schaffung einer gesetzlichen Grundlage für die Verwendung der AHVN13 anstrebt;
2. die Schaffung eines bereichseigenen Personenidentifikators plant oder
3. die Identifizierungsarbeit manuell durchführen will.

Die im nachfolgenden Kapitel beschriebenen Fallbeispiele zeigen auf, dass die Nichtverwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators mit Risiken und Kosten verbunden ist.

4 Fallbeispiele

Für die Erhebung der Fallbeispiele wurden einstündige Interviews mit IT-, Bereichs- und Geschäftsverantwortlichen der entsprechenden Behörden geführt[6]. Es handelt sich dabei um einige wenige Beispiele zur Illustration der Herausforderungen und Risiken. Es übersteigt die Möglichkeiten dieses Gutachtens, die grosse Zahl aller analogen Fälle aufzuzeigen. Die Fallbeispiele beschreiben

[5] Botschaft zum Strafregistergesetz vom 20. Juni 2014 (SR 14.053), Botschaft zur Änderung des Obligationenrechts (Handelsregisterrecht) vom 15. April 2015 (SR 15.034), Botschaft zur Änderung des Schweizerischen Zivilgesetzbuches (Beurkundung des Personenstands und Grundbuch) vom 16. April 2014 (SR 14.034)

[6] Die Liste der Interviewteilnehmenden befindet sich im Anhang.

Schwierigkeiten der in Erfüllung ihres gesetzlichen Auftrages handelnden Behörden, welche sich bei der Identifikation von Personen ergeben.

4.1 Mehrwertsteuerunterstellung bei Einzelfirmen

4.1.1 Ausgangslage und Beschreibung des Fallbeispiels

Die Hauptabteilung Mehrwertsteuer bei der Eidgenössischen Steuerverwaltung ESTV ist für die korrekte Erhebung der Mehrwertsteuer und deren Einzug zuständig [11].

Bei Einzelfirmen werden Personen, nicht Unternehmen, registriert. Bei Restaurantbetrieben beispielsweise kommt es oft vor, dass die eingetragene Person Konkurs geht. Zu bemerken gilt, dass hierbei nicht die Einzelfirma, sondern eben die eingetragene Person betroffen ist. Falls diese Person dann einen neuen Betrieb eröffnen will, ist es sehr schwierig herauszufinden, ob diese Person in irgendeinem Zusammenhang noch unbezahlte Posten hat.

Illustration. Herr Meier betreibt das Restaurant Rössli. Der Mehrwertsteuerbehörde fällt auf, dass Herr Meier für seinen Betrieb keine Mehrwertsteuer abgerechnet hat. In der Zwischenzeit hat aber Herr Meier seinen Betrieb geschlossen. Er kann seine offene Mehrwertsteuerrechnung nicht bezahlen. Es wird ein Konkursverfahren gegen ihn eingeleitet. Derselbe Herr Meier übernimmt nun mit dem Restaurant „zum Löwen“ einen anderen Restaurantbetrieb und meldet seinen Betrieb bei der Mehrwertsteuerbehörde an. Die Mehrwertsteuerbehörde nimmt die Anmeldung an, ohne zu wissen, dass Herr Meier bei ihnen offene Posten hat.
Aktuell ist es für die Mehrwertsteuerbehörde sehr aufwändig, solche Fälle zu verhindern. Solche Fälle generieren für die Mehrwertsteuerbehörde einen ganz konkreten finanziellen Schaden.

Eine besondere Herausforderung für die Mehrwertsteuerbehörde stellt sich auch in Fällen, in denen eine Person mehrere Firmen besitzt. Diese Firmen können unterschiedliche Rechtsformen aufweisen. Im Rahmen der Bearbeitung eines Dossiers sieht die Mehrwertsteuerbehörde nicht, ob diese Person in einem anderen Fall noch offene Schulden hat.

Rückerstattungen
Die Rückerstattung der Verrechnungssteuer für ausländische Staatsangehörige erfolgt auf Bundesebene. Diese fordern formularbasiert die Rückerstattung ihrer Steuer ein. Auch hier ist es für die Steuerbehörde sehr aufwändig zu erkennen, ob diese Person noch offene Posten bei der Steuerbehörde hat. Deshalb ist bei Rückerstattungen an ausländische Staatsangehörige die Identifizierung sehr wichtig.

Ähnliche Herausforderungen stellen sich im Bereich Steuerbetrug und im Rahmen des automatischen Informationsaustauschs.

Der Austausch von Informationen im Kontext mit eindeutigen Personenidentifikatoren mit anderen Behörden ist eher gering. Aktuell erhält die ESTV ~~nur~~ Daten aus den Konkursregistern und die UID von Einzelfirmen aus dem UID-Register. Die ESTV selbst übermittelt Steuerdaten an zuständige Ermittlungsbehörden nur im Fall von Strafdelikten. Ein Bedarf nach einem eindeutigen Personenidentifikator besteht vor allem bei Verwaltungsabläufen innerhalb der ESTV.

4.1.2 Konsequenzen eines Nichteinsatzes der AHVN13

Allein im Rahmen der Mehrwertsteuerunterstellung von Einzelfirmen kann ein finanzieller Schaden in Millionenhöhe entstehen.

Die Erfolgswahrscheinlichkeit bei der eindeutigen Identifikation von Personen ist aktuell sehr gering. Die Identifikation mittels Nachnamen und Geburtsdatum ist heute nicht mehr eindeutig. Ein Teil des Problems liegt darin, dass in der Schweiz Namen veränderbar sind. Folglich bleibt, bis auf die AHVN13, in der Schweiz keine Konstellation mehr, die die eindeutige Identifikation einer Person erlauben würde.

In vielen heutigen Prozessen bei der ESTV ist eine fachliche Überprüfung der Gesuche eingebaut. Konkret werden die eingereichten Formulare einem Sachbearbeitenden zugewiesen. Dieser klärt ab, ob der unterstellten Person bereits etwas ausbezahlt wurde oder ob mehrere Anträge für diese Person offen sind. Diese Abklärungen erfolgen manuell und erschweren den Bearbeitungsprozess massgeblich. Der oder die Sachbearbeitende muss in einer Datenbank mit ca. 600‘000 Personen / Unternehmen manuell nach Redundanzen suchen.

Die hier beschriebene Herausforderung, vor der die ESTV bei der Erfüllung ihres gesetzlichen Auftrages steht, ist auch bereits im Rahmen der regelmässigen Überprüfungen der Eidgenössischen Finanzkontrolle EFK Thema [12]. Sie gibt beispielsweise in ihren Berichten zu bedenken, dass bei Auszahlungen das Risiko besteht, dass der Betrag an dieselbe Person doppelt bezahlt werden könnte. Heute lässt sich dies nur anhand des Auszahlungskontos überprüfen. Die ESTV setzt organisatorische, statt technische, Massnahmen ein, um den Forderungen der EFK nachzukommen.

4.1.3 Aktuelle Tätigkeiten und Ausblick

Die oben erwähnten Probleme tauchen in fast allen Inkasso- sowie Rückzahlungsprozessen auf. Deshalb ist der Einsatz von Systemen vorgesehen, die eine Effizienzsteigerung von ca. 30-40% erlauben. Es handelt sich dabei um Matching-Software. Auf all diese Massnahmen könnte verzichtet werden, wenn ein eindeutiger Personenidentifikator vorhanden wäre.

Die Erhebung von Personendaten erfolgt heute gestützt auf der Selbstdeklaration der betroffenen Person. Neu wird die ESTV die AHVN13 bei neuen Mehrwertsteuerunterstellungen abfragen.

Hier können Diskussionen zur Gesetzmässigkeit dieser Handlung entstehen. Die Unsicherheit, die sich stellt, liegt nicht bei der Abfrage der Nummer, sondern bei deren Verwendung. Die Rechtmässigkeit bei Datenverknüpfungen ist nicht immer offensichtlich. Es ist anhand der heutigen Gesetzgebung nicht eindeutig ersichtlich, ob es z.B. zulässig ist, für die Bearbeitung eines Rückerstattungsfalles, Informationen aus dem Mehrwertsteuerbereich zu berücksichtigen. Obwohl die gesetzlichen Grundlagen existieren, ist die konkrete Auslegung der bestehenden Gesetze unklar.

Aus Sicht der Steuerverwaltung besteht ein klarer Bedarf nach einem Personenidentifikator. Wie dieser Identifikator ausgestaltet ist, spielt keine Rolle. Für den Steuerbereich wäre es denkbar, eine Steuernummer für alle Personen, die der Bundessteuer unterstellt sind, einzuführen.

Die Forderung nach der Verwendung der AHVN13 als eindeutiger Personenidentifikator ist aus Sicht des automatischen Informationsaustauschs zudem zu stark an nationale Grenzen gebunden. Der internationale Aspekt wird damit völlig ausgeblendet. Welche Nummer ein Land als Identifikator verwendet, sollte im internationalen Kontext geregelt werden. Die Kriterien für diese Nummer müssen international vereinbart werden. Dabei könnte z.B. die AHVN13 für die Schweiz als international anerkannter Personenidentifikator verwendet werden.

4.2 Fallbeispiel Grundbuch

4.2.1 Ausgangslage und Beschreibung des Fallbeispiels

Die schweizerischen Grundbücher sind grundstücksbezogen aufgebaut. Es besteht kein zentrales Grundbuch für die ganze Schweiz. Die Eigentümerschaft der Grundstücke werden bei Bedarf (z.B. bei Erbschaften, Vermögenssperre von Potentaten) mit einem Hilfsregister (bzw. mit einer Liste der Grundbuchämter) ermittelt, das nach Gemeinden oder Grundbuchkreisen geführt wird [13]. Für die einheitliche Erfassung von u.a. Personendaten in allen Grundbüchern hat das Bundesamt für Justiz BJ im Jahre 2011 ein Datenmodell [14] verabschiedet. Dieses Datenmodell ist heute implementiert. Dieses definiert die folgenden Personenmerkmale: Name, Vorname, Geburtsdatum, Geschlecht, Heimatort oder Staatsangehörigkeit. Die Erfassung der Personendaten erfolgt jeweils zum Zeitpunkt des Grundstückkaufs. Es erfolgt oft keine Aktualisierung der Daten, da im Grundbuch das

Antragsprinzip gilt, wonach Daten nur auf Antrag der Betroffenen verändert werden dürfen. Seit dem 1.1.2012 werden die Personalien anhand einer Pass- oder ID-Kopie überprüft (Art. 51 GBV).

Heute ist es nicht möglich zu sehen, auf welche Grundstücke in der Schweiz eine Eigentümerin oder ein Eigentümer ein Recht hat. Soll z.B. in Zusammenhang mit einer Straftat sämtlicher Grundstücksbestand eines Eigentümers ermittelt werden, ist dies heute nur mit grossem Aufwand erzielbar und nicht immer möglich. Die dezentrale Führung des Grundbuchs und das Fehlen einer technischen Infrastruktur erschwert eine landesweite Suche nach Eigentümerschaft massgeblich. Die Suche muss separat bei jedem Grundbuch durchgeführt werden. Zudem erfolgt die Suche gestützt auf die oben erwähnten Personenmerkmale. Weil die Personendaten in den Grundbüchern nicht aktualisiert werden müssen, können die Personendaten von ein und derselben Person – trotz einheitlichem Datenmodell - je nach Register unterschiedlich erfasst sein. Der unterschiedliche Datenstand ist auch Folge der geschichtlichen Entwicklung in der Erfassung dieser Personenmerkmale. Die vollständige Erfassung der Personenmerkmale gemäss oben erwähntem Datenmodell ist erst seit 3-4 Jahren gefordert. Reichte in früheren Zeiten die Angabe des Namens, wurden neu graduell weitere Merkmale, wie z.B. das Geburtsdatum oder der Heimatort, gefordert.

Der unterschiedliche Datenstand führt dazu, dass in einigen Fällen Einträge derselben Person bei unterschiedlichen Registern nicht erkannt werden (keine Erkennung der Übereinstimmung).

Abbildung 2: Nicht erkannte Übereinstimmung

In Abbildung 2 wird ein fiktiver Fall von nicht erkannter Übereinstimmung dargestellt. Frau Verena Müller, geboren am 16. Juni 1967, kauft ein Grundstück im Baselland. Ihr Geburtsdatum gibt sie nicht an. Es wurde zu dieser Zeit noch nicht gefordert. Einige Jahre später möchte Frau Müller nach Bern umziehen und sieht sich einige Eigentumswohnungen an. Sie entschliesst sich für den Kauf einer Eigentumswohnung in der Stadt. Hier gibt sie ihr Geburtsdatum an. In Bern begegnet Frau Müller ihrem jetzigen Ehemann Herr Meier. Sie nimmt bei der Heirat seinen Nachnamen an und verwendet von nun an in allen administrativen Belangen den Namen Verena Meier. Als Folge der Eheschliessung erhält sie Bern als zweiten Heimatort. Danach erwirbt sie noch zwei weitere Grundstücke. Eins im Kanton Zürich und eins im Kanton Tessin. Während sie dem Grundbuchamt in Zürich aus reiner Gewohnheit noch Zürich als ihren Heimatort angibt, nennt sie beim Kauf ihres Grundstücks im Tessin ihren zweiten Heimatort an. Erst die Verwendung eines eindeutigen Personenidentifikators vermag die eindeutige Übereinstimmung dieser Einträge zu gewährleisten.

Abbildung 3: Falsche Übereinstimmung

Weiter können falsche Übereinstimmungen zu Verwechslungen führen. Abbildung 3 zeigt ein mögliches Beispiel einer falschen Übereinstimmung. Dass es sich in diesem Fall nicht um dieselbe Person handelt, ist erst durch die Betrachtung der AHV-Nummer erkennbar.

4.2.2 Konsequenzen eines Nichteinsatzes der AHVN13

Die Fälle von Frau und Herr Müller illustrieren die Schwierigkeiten, die sich bei der Identifikation von Eigentümerinnen und Eigentümern in verschiedenen Grundbüchern ergeben. Ohne einen eindeutigen Personenidentifikator kann die fehlerhafte Übereinstimmung im Falle von Herrn Müller und die nicht erkannte Übereinstimmung im Falle von Frau Müller nicht zuverlässig entdeckt werden. Dieser Umstand erschwert und verunmöglicht teilweise die Ermittlung der Grundstücke, die im Besitz einer bestimmten Person sind. Besonders relevant wird diese Information in Zusammenhang mit einer Straftat.

Die eindeutige Identifikation von Personen ohne Verwendung eines Personenidentifikators kann zu Fehlern und Falschverknüpfungen führen. Um die eindeutige Identifikation von Personen in den Grundbüchern sicherzustellen, bedarf es eines eindeutigen Personenidentifikators.

4.2.3 Aktuelle Tätigkeiten und Ausblick

Die Botschaft zur Änderung des Schweizerischen Zivilgesetzbuches (Beurkundung des Personenstands und Grundbuch) vom 16. April 2014 liegt vor. Sie wurde im Parlament noch nicht behandelt. Darin wird die Führung des Grundbuchs mittels der AHVN13 als Personenidentifikator beantragt [15]. Ziel ist die eindeutige Identifikation von Eigentümern in Grundbüchern. Für den Informationsaustausch mit Stellen, die nicht zur systematischen Nutzung der AHVN13 berechtigt sind, ist die Verwendung eines, von der AHVN13 abgeleiteten sektoriellen Personenidentifikators, vorgesehen. Durch die Verwendung des von der AHVN13 abgeleiteten sektoriellen Personenidentifikators wird die AHVN13 der Eigentümerschaft nicht weitergegeben.

4.3 Fallbeispiel Vereinigung der Strassenverkehrsämter

4.3.1 Ausgangslage und Beschreibung des Fallbeispiels

Die Vereinigung der Strassenverkehrsämter (asa) ist u. a. für die Administration und Registrierung von obligatorischen Ausbildungen für Neulenkende, Chauffeure, Fahrlehrende und Gefahrgutfahrende zuständig.

Beim Erhalt eines Führerausweises wird den Personen eine FABER ID zugeteilt, die sie auf Lebenszeit erhalten und die auf ihrem Führerausweis aufgedruckt wird. Bei der FABER ID handelt es sich um einen eindeutigen Identifikator, der beim Bundesamt für Strassen im FABER (Fahrberechtigungsregister) geführt und für jede Person mit Beantragung ihres Fahrausweises angelegt wird. Der genaue Umfang von FABER kann der Verordnung über das Fahrberechtigungsregister Art.3 entnommen werden [16].
Die FABER ID dient der asa in fast allen Fällen als eindeutiger Identifikator. Es gibt allerdings immer wieder Ausnahmen, in denen die Person nicht zwingend einen Führerausweis hat und somit auch keine FABER ID besitzt. So hat beispielsweise Lehrpersonal für die angebotenen Ausbildungskurse

nicht in jedem Fall einen Führerausweis und kann somit nicht immer über die FABER ID geführt werden.

Des Weiteren gibt es Bestrebungen, dass die asa zukünftig auch die obligatorischen Weiterbildungen für Ärztepersonal (Hausärzte und Verkehrsmediziner) und Psychologinnen und Psychologen verwaltet. Hierbei stellt sich allerdings das Problem, dass nicht zwingend alle Personen im Gesundheitswesen einen Fahrausweis und damit FABER ID besitzt. Um dennoch einen eindeutigen Identifikator in diesem Fällen zur Verfügung zu haben, wurde mit dem Bundesamt für Gesundheit (BAG) vereinbart, dass die GLN (Global Location Number, ehemals EAN), durch die asa verwendet werden darf.
Ebenfalls werden möglicherweise zukünftig Nothelfer-Ausbildungen durch die asa verwaltet. Auch hier gibt es einen Teil der Personen (ca. 20%), die aufgrund ihres Alters noch keinen Fahrausweis und somit auch keine FABER ID besitzen. Für diese Personengruppe existiert aktuell kein eindeutiger Personenidentifikator, sodass hier beispielsweise auf die AHVN13 zugegriffen werden müsste.

4.3.2 Konsequenzen eines Nichteinsatzes der AHVN13

Aus der obigen Beschreibung ist ersichtlich, dass es trotz einer FABER ID immer wieder Ausnahmefälle gibt, bei denen dieser eindeutige Identifikator nicht verwendet werden kann, da eine FABER ID nur Personen mit Fahrausweis besitzen (falls zu einem späteren Zeitpunkt die Person ihren Fahrausweis abgibt, bleibt die FABER ID allerdings bis zum Ableben der Person bestehen).
Kommt es zu solchen Ausnahmefällen, versucht man sich durch weitere IDs (wie z. B. der GLN) zu behelfen, die allerdings auch nur wieder für einen eingeschränkten Personenkreis gelten.
Für einige Ausnahmefälle wie beispielsweise beim Lehrpersonal ohne Fahrausweis kann nur auf die AHVN13 zurückgegriffen werden, da dies der einzige eindeutige Identifikator ist, den alle Personen dieser Gruppe besitzen.

4.3.3 Aktuelle Tätigkeiten und Ausblick

Um für die bestehenden Ausnahmefälle einen generell verwendbaren eindeutigen Identifikator verwenden zu können, unterstützt die asa die Einführung einer AHVN13 als einheitlicher, organisationsübergreifender genutzter Personenidentifikator. Die FABER ID würde allerdings aufgrund des damit verbundenen hohen Aufwands nicht sofort durch die AHVN13 abgelöst. Denkbar wäre eventuell eine kontinuierliche Ablösung über die nächsten Jahrzehnte.

4.4 Fallbeispiel Strassenverkehrsämter der Kantone

4.4.1 Ausgangslage und Beschreibung des Fallbeispiels

Die Strassenverkehrsämter der Kantone greifen auf die Daten der asa zu und nutzen damit auch die FABER ID als eindeutigen Identifikator. Für die Ausstellung der KfZ-Steuern beispielsweise ist es für die Strassenverkehrsämter darüber hinaus sehr wichtig, die aktuelle Adresse der Fahrzeughalterinnen und Halter zu kennen. Da Fahrzeughaltende bei Umzügen die neue Adresse in vielen Fällen den Strassenverkehrsämtern nicht mitteilen, erhalten diese Adressänderungen in der Regel über die Einwohnerkontrollen. Die Strassenverkehrsämter leiten die erhaltenen Informationen an FABER weiter. In der Kommunikation mit FABER beim Bundesamt für Strassen erfolgt die Identifikation der Person über die FABER ID.

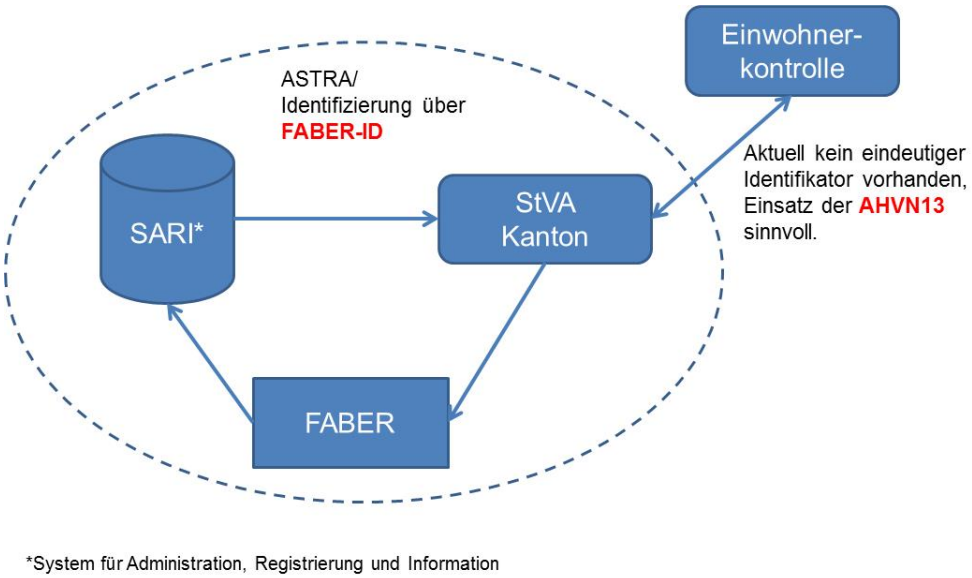

Abbildung 4: Darstellung einer möglichen Verwendung der AHVN13 zur Kommunikation zwischen Einwohnerkontrollen und Strassenverkehrsämtern

4.4.2 Konsequenzen eines Nichteinsatzes der AHVN13

Die FABER ID obliegt dem Bundesamt für Strassen und darf nur von der asa und den Strassenverkehrsämtern der Kantone genutzt werden. Für den Abgleich der Datenbanken zwischen den Strassenverkehrsämtern der Kantone und der jeweiligen Einwohnerkontrolle werden daher die Attribute Name, Vorname und Geburtsdatum verwendet. Falls diese Kombination mehrfach auftritt, muss das jeweilige Strassenverkehrsamt manuell feststellen, welche Person gemeint ist. Dies führt immer wieder zu Aufwänden, die durch die Nutzung einer AHVN13 eliminiert werden könnten.

4.4.3 Aktuelle Tätigkeiten und Ausblick

Die Einführung einer AHNV13 könnte die Kommunikation zwischen Strassenverkehrs- und Einwohnerämtern vereinfachen, indem Adressänderungen über die AHVN13 den betreffenden Personen zugeordnet werden könnten. Aus diesem Grund ist die flächendeckende Nutzung einer AHVN13 in diesem Kontext von Relevanz.

4.5 Fallbeispiel Schifffahrt

4.5.1 Ausgangslage und Beschreibung des Fallbeispiels

Das Bundesamt für Verkehr ist zuständig für Fragestellungen im Zusammenhang mit der Schifffahrt. Die Registrierung der Schiffe wird aber nicht über den Bund verwaltet, sondern in den Strassenverkehrsämtern der Kantone. Jeder Kanton besitzt somit ein eigenes Register und damit auch jeweils einen eigenen eindeutigen Personenidentifikator für Schiffshaltende. Bei einem Umzug in einen anderen Kanton erhält die Halterin oder der Halter des Schiffes jedes Mal einen neuen Identifikator.

4.5.2 Chancen durch einen Einsatz der AHVN13

Die Einführung einer AHVN13 könnte zu einer einheitlicheren Datenverwaltung führen. So würde die Vergabe einer neuen ID-Nummer durch die Nutzung der AHVN13 entfallen und damit der entsprechende administrative Verwaltungsaufwand. Ein Beispiel für die hohen Aufwände, die auf die einzelnen kantonalen Lösungen zurückzuführen ist, ist das Unglück auf dem Bielersee vor einigen Jahren. Hier musste unverzüglich der Halter eines bestimmten Schiffes ausgemacht werden, was

aufgrund der unterschiedlichen involvierten Kantone zu einer entsprechenden Zeitverzögerung geführt hat.

4.5.3 Aktuelle Tätigkeiten und Ausblick

Aktuell sind keine Tätigkeiten geplant. Die Nutzung der AHVN13 könnte allerdings wie oben dargestellt zu einer bedeutenden Vereinfachung führen.

4.6 Fallbeispiel Strafregister VOSTRA

4.6.1 Ausgangslage und Beschreibung des Fallbeispiels

Im Strafregister-Informationssystem VOSTRA (Vollautomatisiertes Strafregister) werden Urteile, Sanktionen und Entscheide gemäss der Verordnung über das Strafregister geführt [17]. Zurzeit sind rund 700‘000 Personen im System verzeichnet. Das Bundesamt für Justiz (BJ) trägt die Verantwortung für VOSTRA. Betrieben und weiterentwickelt wird VOSTRA durch das Informatik Service Center ISC-EJPD. Pro Jahr wird ein Release durchgeführt, das rund 400 Personentage exkl. externer Ressourcen umfasst. Für den Betrieb, unter anderem für die Datenqualität, sind beim BJ fünf Personen beschäftigt. Als Herausforderung für VOSTRA gilt, dass die registrierten Personen (anders als in den vorangehenden Fallbeispielen) oftmals nicht an einer korrekten Identifikation interessiert sind.
In Bezug auf die korrekte Personenidentifikation wurden zwei Fälle identifiziert. Zum einem muss bei einer Einzelabfrage die Person korrekt identifiziert werden. Zum anderen betrifft dies Schnittstellen zu anderen Systemen (teilweise auch von anderen Organisationen), die auf das VOSTRA zugreifen und aufgrund entsprechender Rechtsgrundlagen auch zugreifen dürfen und dabei auf eine korrekte Verknüpfung angewiesen sind.

Aktuell wird das Geschäft „Bundesgesetz über Verbesserungen beim Informationsaustausch zwischen Behörden im Umgang mit Waffen“ [18] im Nationalrat behandelt. Dieses Geschäft schlägt eine Änderung des Strafgesetzbuches vor. Dabei soll ein sicherer, einfacher und eindeutiger Austausch mit dem VOSTRA, basierend auf der AHVN13, ermöglicht werden. Ein Beispiel für den Datenaustausch ist das Personalinformationssystem der Armee (PISA). Die Armee benötigt den Leumund für Rekrutierungen und Beförderungen aus dem VOSTRA. Der Datenaustausch findet periodisch statt und ist teilautomatisiert. Weitere Schnittstellen bestehen ebenfalls teilautomatisiert zu kantonalen Strafjustizen und Bundesregistern (ZEMIS, Infostar). Trotzdem müssen Daten mehrfach in unterschiedlichen Systemen erfasst werden. Der manuelle Abgleich zwischen Systemen und die Bestellung eines Strafregisterauszuges erfolgt anhand von Personenattributen wie Familienname, Geburtsname, Vorname(n), Geburtsdatum, Namen und Geburtsdatum der Eltern und ist entsprechend zeitintensiv und fehleranfällig.

4.6.2 Konsequenzen eines Nichteinsatzes der AHVN13

Eine gewollte oder ungewollte falsche Identifizierung im VOSTRA kann weitgehende Folgen haben. So kann eine Person, unter Angabe von falschen Informationen, unter Umständen einen „leeren“ Strafregisterauszug beziehen. Reziprok wird einer Person ein Strafregisterauszug mit falschen Daten ausgegeben. Beide Fälle gilt es durch eine möglichst gute Personenidentifikation zu verhindern. Eine Identifikation basierend auf den Personenattributen ist nicht ausreichend, da diese über keine Konsistenz verfügen und beispielsweise bei einer Heirat unter Umständen[7] geändert werden oder durch unterschiedliche Schreibweisen nicht vergleichbar sind. Auch die Eindeutigkeit ist, selbst beim Verwenden von mehreren Personenattributen, nicht in allen Fällen gegeben.

Der administrative Aufwand rund um das VOSTRA Register ohne einheitlichen, organisationübergreifenden Personenidentifikator ist schwierig zu beziffern. Auf Seiten des Registers VOSTRA sind mehrere Personen damit beschäftigt, Daten zu bereinigen und Nachforschungen

[7] Neues Namensrecht seit 1.1.2013 - Namenswahl bei Heirat und gleichgeschlechtlicher Partnerschaft. [30]

betreffend Personenidentifizierung durchzuführen. Dies erfolgt durch Abfragen von anderen Registern oder direktem Kontakt mit anderen Behörden. Dies führt auch in anderen Organisationseinheiten zu einem administrativen Mehraufwand, um die oft manuellen Abklärungen zu tätigen.
Der Austausch von Informationen innerhalb der Bundesverwaltung, mit den Kantonen und dem Militär ist sehr aufwändig und fehleranfällig. Dies hat zur Folge, dass ebenfalls aufwandintensive Abklärungen gemacht werden müssen.
Die indirekten Folgen einer falschen Personenzuordnung sind innerhalb dieses Berichtes und den verfügbaren Informationen nicht abschätzbar.

4.6.3 Aktuelle Tätigkeiten und Ausblick

Die Schaffung einer gesetzlichen Grundlage für die Verwendung der AHVN13 ist bereits im Zusammenhang mit der Botschaft 13.109 angestossen worden [18]. Für die Einführung der Versichertennummer nach Artikel 50e AHVG in VOSTRA und die Programmierung einer Schnittstelle zwischen PISA und VOSTRA ist gemäss einer provisorischen Kostenschätzung mit Informatikkosten von ca. 1.9 Millionen Franken zu rechnen. In diesem Betrag enthalten sind u.a. die Kosten für die Erarbeitung eines detaillierten Lösungskonzepts und für die Umprogrammierungsarbeiten. Die aktuelle VOSTRA Infrastruktur wurde im Jahr 2010 entwickelt. Eine Anpassung für die AHVN13 ist sehr aufwändig und zurzeit wird überprüft, ob sich eine Anpassung lohnt oder ob das ganze System abgelöst werden soll. Eine Kostenschätzung für eine Gesamterneuerung liegt noch nicht vor.
Ziel ist es - und dies zeigen auch die Bemühungen des Bundesamts für Justiz - die Prozesse zu vereinfachen und eine sichere Personenidentifikation mittels AHVN13 für das VOSTRA einzuführen.

4.7 Zusammenfassung der Ergebnisse

Bei allen beschriebenen Anwendungsfällen geht es darum, Personen eindeutig zu identifizieren. Dies ist meistens nicht der gesetzlich umschriebene Hauptauftrag, sondern dient lediglich dazu, die richtigen Personen einem fachlichen Fall zuzuordnen. Die Identifikation findet über zur Verfügung stehende Personenattribute (Name, Vorname, Geburtsdatum etc.) oder über einen eigenen Identifikator statt. Diese und weitere Personendaten und Identifikatoren werden zusätzlich in allen beschriebenen Fällen in einem eigenen Register geführt, teilweise aufwändig aktuell gehalten oder gar nicht aktualisiert. Somit werden Daten innerhalb der Verwaltung mehrfach in unterschiedlichen Systemen redundant geführt und gepflegt. Personenattribute eignen sich nur bedingt, um eine eindeutige Identifizierung durchzuführen. Besonders Schnittstellen zwischen Systemen sind auf eindeutige Identifikation angewiesen. Eine Zusammenarbeit über Organisationsgrenzen hinweg wird ohne einen eindeutigen Personenidentifikator als aufwändig beschrieben.

Der administrative Aufwand für eine korrekte Identifizierung fällt bei der direkt betroffenen Stelle sowie bei nachgelagerten Organisationen an. Oft werden bei einer unklaren Zuordnung von einer Person bei verschiedenen Stellen weitere Informationen abgeholt. Dies geschieht bei den meisten beschriebenen Fallbeispielen manuell durch einen Sachbearbeitenden. Diese manuellen Abklärungen und die aufwändige Identifizierung im Allgemeinen führen zu einer langen Durchlaufzeit von Prozessen. Für eine korrekte Identifizierung werden Informationen (Geburtsdatum, Heimatort, Angaben über Eltern, etc.) erhoben, welche für den eigentlichen Geschäftsfall nicht notwendig sind.

Die Verwendung der AHVN13 als Identifikator wird begrüsst. Besonders geschätzt wird die grosse Verbreitung. Die betrachteten Fallbeispiele setzten Lösungen ein, welche vor der Einführung der AHVN13 entwickelt wurden. Ein Nichtverwenden der AHVN13 als Identifikator wird daher als aktueller IST-Zustand beschrieben und als Grund für die aktuellen Probleme bei Datenaustausch und Identifikation genannt.

5 Regelungen im Ausland

Im vorliegenden Projekt wurden neben den Fallbeispielen aus der Schweiz auch die Regelungen im Ausland untersucht. Dabei wurden drei europäische Länder betrachtet, in denen ein eindeutiger

Personenidentifikator bereits flächendeckend im Einsatz ist. Ausgewählt wurden für dieses Projekt die Länder Dänemark, Niederlande und Spanien, weil die Rahmenbedingungen in diesen Ländern etwa mit der Schweiz vergleichbar sind. In allen drei Ländern wurden Experteninterviews per Telefon durchgeführt.

5.1 Das Centrale Personenregister (CPR) in Dänemark

Die Situation in Dänemark wurde mittels Internetrecherche und einem Interview mit Herr Carsten Grage, CPR-Leiter im dänischen Innenministerium, und Herr Rasmus Theede, Vorsitzender des Rates für Digitale Sicherheit, erhoben. Der Rat für Digitale Sicherheit existiert seit drei Jahren und zählte anfangs v.a. Personen aus der Privatwirtschaft in seinen Reihen. Heute sind auch staatliche Institutionen im Rat vertreten. Der Rat gilt in Dänemark als Expertenrat in Sachen Datenschutz und Cybersecurity und wird von den Medien zu diesen sachbezogenen Themen um seine Meinung gefragt.

5.1.1 Infrastruktur und Verwendung des Personenidentifikators

Das Register

Das zentrale Personenregister in Dänemark, kurz CPR, wurde 1968 eingeführt. Die Behörde, die den Betrieb des CPR sicherstellt, ist im Innenministerium angesiedelt. Die gesetzliche Grundlage für das CPR regelt Zweck und Modalitäten der Registerführung (Erfassungs- und Mutationsregeln, sowie die Regeln zur Datenfreigabe an Dritte) [19]. Sie enthält Daten zu sämtlichen Personen mit Wohnsitz in Dänemark und enthält v.a. die folgenden Personenbasisdaten:

- Die *Civil Registration Number* (CPR-Nummer)
- Vollständiger Name
- Aktuelle Adresse
- Nationalität
- Zivilstand
- Geburtsdatum
- Beruf

Das CPR enthält aktuelle Daten, wobei die früheren Daten historisiert zur Verfügung stehen. Aufgrund verschiedener Datenquellen kann es vorkommen, dass eine Person doppelt erfasst wird. Es handelt sich jedoch um eine marginale Erscheinung.

Die Registerquellen

Personen mit Wohnsitz in Dänemark müssen sich bei der Behörde ihres Wohnsitzes registrieren. Entsprechend sind die lokalen und kommunalen Behörden zu den Hauptdatenquellen des CPR zu zählen. Weitere Datenquellen sind die Kirchen, die Spitäler und das Justizministerium. So werden z.B. Geburten oder Todesfälle direkt vom Spital aus im System erfasst.

Die Weitergabe der Daten

Grundsätzlich können CPR-Daten an alle Behörden weitergegeben werden. Bei der Weitergabe der Daten an Behörden erfolgt eine Initialprüfung. Dabei verpflichtet sich die anfragende Behörde, das Gesetz über die Datenverarbeitung [20] einzuhalten, und die Modalitäten der Datenübermittlung werden festgelegt. Die Behörde kann auf jede Information aus dem CPR-System zugreifen, die sie zur Ausübung ihrer Tätigkeit benötigt. Die Einhaltung des relevanten Datenschutzgesetzes liegt in der Verantwortung des Datennutzers.

Die Weitergabe von CPR-Daten an Private folgt der gleichen Logik. Das Unternehmen verpflichtet sich, das Gesetz über die Datenverarbeitung einzuhalten und legt vertraglich die Modalitäten der Datenübermittlung fest. Die Datenweitergabe ist erlaubt, sofern diese folgende Angaben zum angeforderten Datensatz vorweisen können:

- Name und Geburtsdatum; oder
- Name und Adresse; oder
- Name und CPR-Nummer.

Nach Angabe dieser Personenmerkmale werden die CPR-Daten an das betroffene Unternehmen freigegeben.

Private Unternehmen erhalten vom CPR jeweils nur den Namen und die Adresse von Personen, die keinen Schutz angefordert haben (siehe nachfolgender Abschnitt). Weiter erhalten sie die Information über den Tod einer Person und darüber, ob die Person wünscht, nicht zu Marketingzwecken kontaktiert zu werden. Eine technische Lösung wurde integriert, um sicherzustellen, dass private Unternehmen nur genau diese Informationen aus dem CPR erhalten.

Eine Person kann den Schutz ihrer Daten verlangen. Folgende Schutzmöglichkeiten sind vorgesehen:

a) Schutz vor Weitergabe der Daten zu Marketingzwecken
b) Schutz vor Weitergabe der Daten zu statistischen und Forschungszwecken
c) Schutz vor Weitergabe der Daten für Einträge in physischen öffentlichen Verzeichnissen
d) Schutz vor Weitergabe der Daten im Allgemeinen

Wird der allgemeine Schutz gemäss Punkt d) beantragt, werden die betroffenen Personendaten für die Dauer eines Jahres für Private nicht freigegeben. Dieser Antrag kann ohne Begründung gestellt werden. Zurzeit machen ca. 40‘000 – 50‘000 Personen von diesem Recht Gebrauch. Der Schutz verfällt nach einem Jahr und muss dann neu beantragt werden. In Sonderfällen kann, unter Angabe eines bestimmten Grundes, dieser Schutz für mehrere Jahre gewährt werden. Diese Schutzklausel wurde am 1. Mai 2014 erweitert. Neu kann die aktuelle Adresse einer Person, in Spezialfällen und aufgrund eines polizeilichen Beschlusses, aus dem CPR gelöscht werden.
Der in Punkt c) beschriebene Schutz hat durch den Einzug der Online-Verzeichnisse an Bedeutung verloren. Der in Punkt b) beschriebene Schutz wurde von ca. 800‘000 Personen, also ca. 20% der Gesamtbevölkerung, in Anspruch genommen. Um die Aussagekraft der dänischen Statistik zu stärken, wurde die Möglichkeit, diesen Schutz zu beantragen, per 1. April 2014 aufgehoben und der Schutz für die betroffenen ca. 800‘000 Personen gelöscht.

Die Authentifizierung bei Online-Diensten erfolgt mittels NEM-ID. Die NEM-ID ist ein One-Time-Password-System, das sowohl für die Nutzung von privaten wie staatlichen Online-Diensten verwendet wird. Für die Registrierung ist die CPR-Nummer erforderlich. Einmal registriert, erhält die NEM-ID-Kontoinhaberin oder der Kontoinhaber jedes Mal, wenn sie oder er sich für ein Service authentifizieren will, ein neues Passwort.

5.1.2 Finanzieller und gesellschaftlicher Nutzen des Personenidentifikators

Der Nutzen des Systems wurde nie quantifiziert. Insgesamt wird der Nutzen in einem immensen Effizienzgewinn und in erhöhter Datenqualität und damit auch Datensicherheit im Bereich Personendaten bewertet. Das CPR-System wird vom ganzen öffentlichen und einem Grossteil des privaten Sektors genutzt. Aktuell verfügen ca. 32‘000 User über einen direkten Zugriff auf das System und jede Nacht werden 340 Auszüge daraus gezogen. Grosse Kunden aus dem Privatsektor sind v.a. Banken, Versicherungen, Telekommunikationsanbieter und Anwältinnen oder Anwälte.

Illustrativ wird die Kette der Transaktionen bei Geburten und im Todesfall beschrieben. Geburten werden direkt von der Hebamme ins CPR-System erfasst. Nur einige Minuten nach der Geburt wird diese Information den zuständigen Behörden übermittelt. Gestützt auf diese Information können Fremdbetreuung- und Gesundheitsdienstleistungen bereits am nächsten Tag beantragt werden. Auch bei einem Todesfall kann das Ereignis direkt im Spital im System erfasst werden. Noch in derselben Nacht wird die Information in sämtliche, ans System angeschlossene Datenbanken übermittelt. Die entsprechend notwendigen Schritte, wie beispielsweise die Sozialhilfeleistungen abzubrechen, die Bankkonten zu sperren oder die Lebensversicherung auszuzahlen, können sofort eingeleitet werden.

Die Zahl der Datentransaktionen ist sehr hoch. Sie wäre ohne CPR gleich hoch. Das CPR-System generiert keine neuen oder zusätzlichen Datentransaktionen. CPR hilft nur, die Abläufe dieser Transaktionen effizienter zu gestalten und die Datenqualität und damit die Datensicherheit zu erhöhen.

5.1.3 Die CPR-Nummer aus Sicht des Datenschutzes

In der dänischen Gesellschaft besteht ein grosser Konsens bezüglich des Nutzens des CPR-Systems. Eine Diskussion kann darüber geführt werden, ob eine bestimmte Behörde die Informationen einer anderen Behörde verwenden darf oder nicht. Dies ist aber eine Diskussion, die auch ohne das Bestehen eines CPR-Systems geführt werden muss. Das CPR-System kann lediglich eine Vereinfachung der Weitergabe dieser Informationen erwirken.

Das Personenregister CPR enthält kaum sensible Daten. Die CPR-Nummer ist nur ein Attribut, das zur eindeutigen Identifikation von Personen dient. Sie ist kein Authentifizierungsmittel, d.h. sie berechtigt nicht zum Zugang auf persönliche Daten aus beispielsweise dem Sozialversicherungs- oder Gesundheitsbereich. Anhand der CPR-Nummer kann noch nicht auf Gesundheitsdaten oder Sozialversicherungsdaten zugegriffen werden. Aus persönlicher Sicht des Interviewten könnte die CPR-Nummer sogar öffentlich gemacht werden. Die Nummer hat seiner Ansicht nach per se keinen Schutzwert.

Massnahmen für die Gewährleistung des Datenschutzes wurden auf legislativer wie auf technischer Ebene getroffen. Auf technischer Ebene sind die Sicherheitsanforderungen nach *best practice* umgesetzt worden. Die gesetzliche Grundlage stützt sich auf zwei Gesetze: das CPR-Gesetz und das Datenverarbeitungsgesetz.

Der Rat der Digitalen Sicherheit sieht Handlungsbedarf im Bereich Datenschutz und Datensicherheit [21]. Grosse Sorge bereiten vor allem Fälle von Identitätsdiebstahl. Kleinkriminelle holen sich Angaben zur Person (inkl. CPR-Nummer) aus Briefkästen. Diese Angaben verwenden sie dann, um im Namen des Nummerninhabers Dienstleistungen zu beziehen oder Transaktionen auszuführen. Eine weitere Sorge bereitet die Nutzung der CPR-Nummer als Authentifizierungsmittel. Wird dies erlaubt, so ist es möglich, allein durch die Angabe der CPR-Nummer auf persönliche Daten des Nummerninhabers zuzugreifen.

5.1.4 Empfehlungen an die Schweiz

Das System hat sich stark bewährt und bringt einen enormen Nutzen für die effiziente Abwicklung von Behördentransaktionen. Estland und andere Länder in Osteuropa haben sich nach dem Kalten Krieg das System in Dänemark zum Vorbild gemacht und dasselbe System umgesetzt. Sämtliche skandinavischen Länder verfügen über ein ähnliches System. In Schweden, wie auch in Estland ist die Nummer, die als eindeutiger Identifikator verwendet wird, öffentlich zugänglich.

Um die Sicherheit der Daten rund um den eindeutigen Personenidentifikator, die CPR-Nummer, zu gewährleisten, wird empfohlen, den Datensatz im zentralen Personenregister möglichst schlank zu halten. Am besten sollten in dieser Datenbank keine sensiblen Daten aufbewahrt werden. Dieser Empfehlung schliesst sich auch der Rat der Digitalen Sicherheit an. Es ist ratsam, Identitätsdaten getrennt von den anderen Daten aufzubewahren. Weitere Empfehlungen des Rates der Digitalen Sicherheit sind:

- Klare Regeln in Bezug auf Authentifizierung verabschieden;
- Die Möglichkeit eröffnen, einmal vergebene Nummern zu wechseln (z.B. im Fall von Identitätsdiebstahl)
- Eine nicht-sprechende Nummer einsetzen, d.h. keine Nummer verwenden, die Rückschlüsse auf Personenangaben wie Alter oder Geschlecht zulässt;

- Privacy Impact Assessments[8] und Privacy Enhancing Technologies[9] einsetzen.

5.2 Die Burgerservicenummer (BSN) in den Niederlanden

Um die Situation in den Niederlanden zu erheben, wurden Internetrecherchen und ein Telefoninterview mit Herrn Uijl Kees, Verantwortlicher für die BSN, Innenministerium, durchgeführt.

5.2.1 Infrastruktur und Verwendung der Personenidentifikators

Das Register

Die *Burgerservicenummer (BSN)* wurde im Jahre 2007 eingeführt [22]. Sie ersetzt die bisherige Sozialversicherungs- und Steuernummer (*SoFi number*). Die Ersterfassung erfolgt heute auf der Gemeinde. Alle Personen, die länger als 4 Monate in Holland verweilen, müssen sich bei der Gemeinde registrieren. Hierfür ist ein gültiger Pass und eine Geburtsurkunde vorzulegen sowie eine angemessene Wohngelegenheit nachzuweisen. Auch für im Ausland wohnhafte niederländische Staatsbürgerinnen und –bürger wird eine BSN geführt.

Die BSN ist auf dem Pass, der Identitätskarte und dem Führerausweis aufgedruckt. Es handelt sich um eine persönliche Nummer.

Die erfassten Personendaten werden im *Basisregistratie personen,* kurz *BRP,* zentral geführt.

Im BRP werden folgende Personendaten geführt [23]:
- Name, Vorname, Geburtsdatum, Geburtsort, Geburtsland
- Informationen zu den Eltern
- Informationen zu Kindern
- Zivilstand
- Nationalität, Aufenthaltsstatus
- Wohnadresse
- BSN

Die Registerquellen [23]

Als Hauptquellen dienen zwei Datenbanken: ein Register, das Informationen zu sämtlichen holländischen Staatsangehörigen enthält, und ein Register, das Informationen zu sämtlichen in den Niederlanden wohnhaften, ausländischen Staatsangehörigen enthält.

Eine registrierte Person kann die Änderung, Korrektur oder Vervollständigung ihrer Daten bei der Einwohnerkontrolle ihrer Gemeinde beantragen. Für die Richtigstellung ihrer Daten muss die Person bei der Einwohnerkontrolle persönlich vorsprechen, ihre Identität und die Korrektheit ihrer Forderung nachweisen, z.B. mittels einer Wohnsitzbescheinigung oder einer Heiratsurkunde.

Die Weitergabe der Daten [24]

Eine gesetzliche Grundlage regelt die Weitergabe der BSN im staatlichen Bereich. Behörden, die Daten aus dem BRP für die Erfüllung ihres gesetzlichen Auftrages benötigen, erhalten die notwendigen Daten unentgeltlich. Behörden, die BRP-Daten nutzen, sind z.B. die Steuer-, Zoll- oder Sozialversicherungsbehörden. Seit dem 1. Juni 2009 ist die BSN bei der Weitergabe von Patienten- oder Kundeninformationen im Gesundheitsbereich per Gesetz verlangt. Die Nummer wird auch im Ausbildungsbereich genutzt.

[8] Ein Evaluationsbericht, der die Einhaltung der Datenschutzvorgaben prüft und Empfehlungen abgibt.

[9] Ein Set von IT-Tools, IT-Applikationen und Mechanismen bzw. ein Set von IT-Massnahmen, die in Online-Dienstleistungen und IT-Fachapplikationen eingebaut werden und den Datenschutz von personenbezogenen Informationen innerhalb dieser Dienstleistungen bzw. Fachapplikationen erlauben.

Jede Verwendung der BSN im privaten Sektor bedarf einer gesetzlichen Grundlage.

Es ist möglich, mittels Gesuch die Freigabe seiner Personendaten an Unternehmen und Private zu unterbinden.

5.2.2 Finanzieller und gesellschaftlicher Wert des Personenidentifikators

Die BSN wird als unverzichtbares Element für die Erhöhung der Qualität von staatlichen Dienstleistungen angesehen. Sie erlaubt einen zuverlässigen und effizienten (gesetzlich erlaubten) Informationsaustausch zwischen Behörden. Zudem ermöglicht sie die einmalige Erfassung von Daten für die Verwendung in staatlichen Verwaltungen. Gesetzlich erlaubte Datenübermittlungen zwischen Behörden werden damit massiv erleichtert bzw. reduziert.

5.2.3 Das Register aus Sicht Datenschutz

Die Bekämpfung von Identitätsdiebstahl wird explizit als eine der Gründe für die Einführung der BSN genannt. Insofern wird die Einführung der Nummer eher als datenschutz*fördernd* betrachtet. Die Weitergabe der BSN wird den Nummerninhaberinnen und Inhabern gesetzlich untersagt. Sie ist als persönliche Nummer zu betrachten, die es zu schützen gilt [22].

Die gesetzlichen Grundlagen zur Gewährleistung des Datenschutzes im Zusammenhang mit der Verwendung des BSN sind das BRP-Gesetz und das Datenschutzgesetz.

Für den gesetzlich erlaubten Informationsaustausch zwischen Behörden ist die Verwendung der BSN zwingend. Damit soll die Zuverlässigkeit und die Qualität der Daten erhöht werden.

5.3 Das Register der Documento Nacional de Identidad (DNI) in Spanien

Die Situation in Spanien wurde mittels Internetrecherche und einem Interview mit Herrn Carlos Gómez Muñoz, Head of the Electronic Identification Unit im ICT-Direktorat im spanischen Ministerium für Finanzen und öffentliche Verwaltung, erhoben.

5.3.1 Infrastruktur und Verwendung der Personenidentifikators

Das Register

Als Personenidentifikator wird in Spanien die Nummer der Identitätskarte (Documento Nacional de Identidad DNI) verwendet. Diese Karte und das dazugehörige Register wurde 1944 beschlossen und in den darauf folgenden Jahren implementiert. Seither wurden verschiede Änderungen an der Karte vorgenommen, u.a. ein zusätzlicher Einbau von elektronischen Funktionen.
Die spanische Polizei ist für den Betrieb des Registers zuständig. Die gesetzlichen Grundlagen für die DNI regeln den Zweck und die Registerführung (Erfassungs- und Mutationsregeln, sowie die Regeln zur Datenfreigabe an Dritte). Für spanische Bürgerinnen und Bürger über 14 Jahre mit Wohnsitz in Spanien ist der Besitz einer DNI verpflichtend, weitere Personen können eine DNI freiwillig erhalten.

Die DNI enthält die folgenden Personenbasisdaten [25] zu sämtlichen Bürgerinnen und Bürgern über 14 Jahren mit Wohnsitz in Spanien:

- DNI Nummer
- Vollständiger Name
- Aktuelle Adresse
- Zivilstand
- Geburtsdatum
- Nationalität
- Geburtsort

- Name der Eltern

Die Personennummer wird auch als Steuernummer (Número de Identificación Fiscal NIF) und auf dem Fahrausweis verwendet. Ausländische Personen erhalten eine Steuernummer (Número de Identidad de Extranjero). Da die Nummer nur spanische Staatsangehörige ab 14 Jahre erfasst, werden für die Sozialversicherungen und für das Gesundheitswesen sektorspezifische Identifikatoren benutzt.

Die Registerquellen

Personen mit Wohnsitz in Spanien müssen sich bei der Behörde an ihrem Wohnsitz registrieren. Die Angaben aus dieser Registrierung müssen dann der Polizeibehörde gemeldet werden. Im Falle einer Adressänderung lässt sich dies auch online erledigen, indem der Polizeibehörde Zugriff auf die Adressdaten aus dem Statistikregister gewährt wird, das die Adressänderung von den lokalen Behörden mitgeteilt erhält.

Die Weitergabe der Daten

Grundsätzlich können DNI-Daten an alle Behörden weitergegeben werden. Nachdem die Behörde einen initialen administrativen Prozess durchlaufen hat, kann sie über einen Broker-Service aufgrund der DNI die registrierten Personendaten erhalten. Voraussetzung dafür ist entweder die Einwilligung der Bürgerin oder des Bürgers, dass ihre oder seine Personendaten bezogen werden dürfen oder das Bestehen einer gesetzlichen Grundlage für den Bezug (z.B. bei Verdacht auf Betrug).

Die DNI wird von vielen Privaten als sekundäres Identifikationsmerkmal erhoben und verwendet, Private haben aber keinen Zugriff auf das staatliche Register.
Für ein Online-Wettangebot wird dem privaten Anbieter eine Altersüberprüfung mittels DNI zur Verfügung gestellt, die aber keine Personendaten enthält.

5.3.2 Finanzieller und gesellschaftlicher Wert des Personenidentifikators

Der Nutzen des Systems wurde nie quantifiziert, da der Identifikator bereits seit Beginn der Informatisierung der Verwaltung zur Verfügung steht. Effizienz im behördenübergreifenden Austausch von Daten (z.B. bei Umzug in eine andere Provinz) sowie eine gute Datenqualität stehen im Vordergrund.
Die Beschränkung, dass der Personenidentifikator nur für spanische Bürgerinnen und Bürger über 14 zur Verfügung steht, führt dazu, dass weitere Identifikatoren notwendig sind. Zur Vereinfachung der Prozesse wurde die Ausstellung eines Personenidentifikators ab Geburt beschlossen. Dieser Prozess wird gegenwärtig implementiert. Aus diesem Personenidentifikator kann dann die DNI abgeleitet werden.

5.3.3 Die DNI-Nummer aus Sicht Datenschutz

Die Verwendung der DNI ist durch die lange Geschichte gut in der Bevölkerung verankert. Die Nutzung einer Identifikationsnummer führt nicht zu spezifischen Problemen im Datenschutz. Die gesetzliche Regelung schreibt vor, dass Bürgerinnen und Bürger Besitzer ihrer Daten sind und dass diese nicht ohne Einwilligung weitergegeben werden dürfen. Damit wird unabhängig vom Identifikator eine Nutzung über verschiedene Datensammlungen ohne Zustimmung des Nummerninhabers untersagt.
Die Amtsstellen, die die DNI verwenden, verpflichten sich, die Datensicherheit zu gewährleisten und die Nummer nicht als einziges Authentifizierungsmittel zu akzeptieren.

5.3.4 Empfehlungen an die Schweiz

Die Wahrnehmung der Nummer durch die Bürgerinnen und Bürger ist entscheidend. In Spanien ist das System sehr bewährt und wird als nützlich und benutzerfreundlich wahrgenommen. Es wurden damit auch keine schlechten Erfahrungen gemacht. Die Einwilligung der Bürgerinnen und Bürger in die Nutzung der Daten schafft Vertrauen.

5.4 Zusammenfassung

Die drei Beispiele aus dem europäischen Raum zeigen, dass ein eindeutiger Personenidentifikator sehr unterschiedlich im Einsatz ist und auch sehr unterschiedliche Historien aufweist. Während die Niederlande einen sehr jungen Personenidentifikator im Einsatz haben (BSN ist seit 2007 im Einsatz), gibt es das CPR in Dänemark bereits seit bald 50 Jahren und Spanien nutzt die DNI, die sogar über 70 Jahre alt ist.
In allen drei Ländern werden nur die wichtigsten Personenbasisdaten in dem jeweiligen Register gespeichert. Somit existieren in den jeweiligen Registern nur wenige (oder keine) sensible Daten, wodurch eine gewisse Datensicherheit gewährleistet ist.
Während Spanien einen eindeutigen Personenidentifikator bisher nur für Personen ab 14 Jahren vorsieht und auf spanische Bürgerinnen und Bürger beschränkt (Änderung vorgesehen), kommt der eindeutige Personenidentifikator in Dänemark und den Niederlanden für alle Personen mit Wohnsitz im jeweiligen Land zum Einsatz, unabhängig von ihrer Nationalität.
Die Komplexität der dahinter liegenden Systeme ist in den drei Ländern teilweise sehr unterschiedlich. So gibt es in Dänemark verschiedene Datenquellen wie Behörden, Kirchen, Spitäler und Justizministerien. In den Niederlanden und Spanien beschränken sich die Datenquellen auf Behörden.

In allen Ländern wird die Verwendung des eindeutigen Identifikators als grosser Nutzen gesehen, der zu einer hohen Effizienz in der Verwaltung beiträgt. Allerdings wird von den Interviewpartnern aus Dänemark und Spanien auf die Gefahren von Identitätsmissbrauch hingewiesen. Im Interview mit den Niederlanden wurde interessanterweise der eindeutige Identifikator als Gegenmittel zum Identitätsmissbrauch betrachtet.

Für die Schweiz lässt sich aus diesen Beispielen entnehmen, dass die Verwendung eines eindeutigen Personenidentifikators einen grossen Nutzen hinsichtlich der Effizienzsteigerung in der Verwaltung darstellt. Das entsprechende Register beschränkt sich auf die wichtigsten Personenbasisdaten. Datenschutz und Cybersecurity ist ein wichtiges Thema, das immer mehr an Bedeutung gewinnt. Dieses steht allerdings einer Einführung eines Personenidentifikators nicht im Wege.

Wichtig ist, vor Einführung eines Personenidentifikators, analog zu den drei Ländern, die gesetzliche Grundlage und Regularien zur Verwendung und Nutzung des Personenidentifikators zu schaffen.

Abschliessend lässt sich sagen, dass der eindeutige Personenidentifikator in den Ländern sehr unterschiedlich zum Einsatz kommt, der grosse Mehrwert in der Effizienzsteigerung innerhalb der Verwaltung aber unbestritten gesehen wird.

6 Analyse und gesamthafte Betrachtung

In diesem Kapitel werden die Ergebnisse aus den Fallbeispielen und den Regelungen im Ausland einer gesamthaften Betrachtung unterzogen und analysiert. In einem ersten Schritt werden die Systeme im untersuchten Ausland mit dem AHVN13-System in der Schweiz verglichen. Danach wird der unterschiedliche Umgang mit dem Datenschutz besprochen, sowie die Unterschiede mit den Fallbeispielen aus der Schweiz analysiert. In den weiteren Schritten wird der Fokus wieder auf die Schweiz gelegt. Die Risiken und die Kosten, die sich aus der aktuellen Situation ergeben, werden gesamthaft betrachtet, um abschliessend eine Synthese der Analyse zu liefern.

6.1 Vergleich mit dem Ausland

Die Interviews mit den Experten im Ausland zeigen, dass die Verwendung eines nationalen, eindeutigen Personenidentifikators mit dem Datenschutz vereinbar ist. Die Verwendung dieser Nummer ist jeweils in einem System eingebettet, das aus einem zentralen Personendatenregister besteht und hauptsächlich auf zwei Gesetzen ruht: einem Registerführungsgesetz und einem Datenschutzgesetz. Abbildung 5 zeigt ein Modell, das die im System eingebetteten Datenbanken (blau) und die dazugehörigen gesetzliche Grundlagen (grün) illustriert. Das Registerführungsgesetz regelt, welche Daten im Register geführt werden, wann eine Mutation zulässig ist, und an wen und

unter welchen Bedingungen die Daten weitergegeben werden dürfen. Es legt auch fest, wann die Weitergabe der Daten zum Schutz der Persönlichkeit untersagt ist.

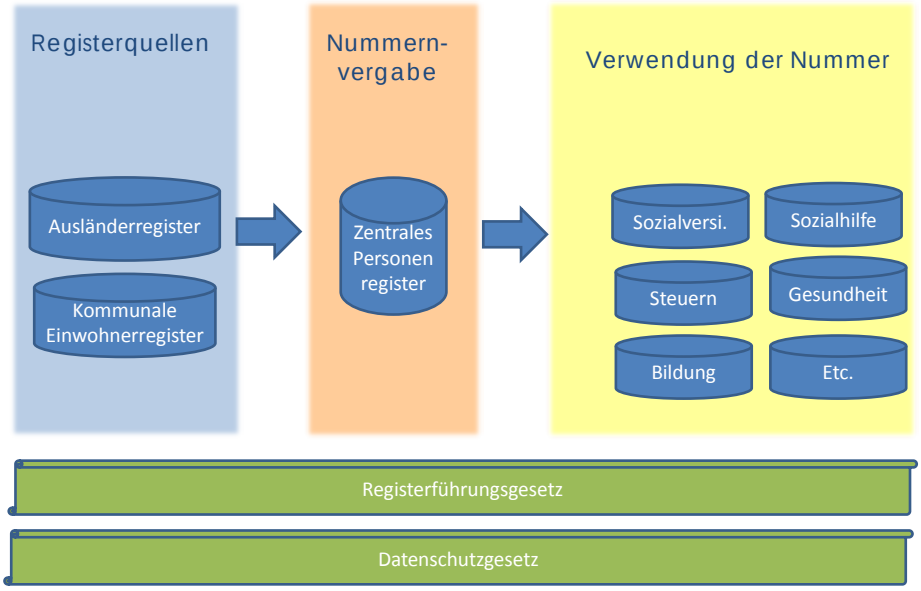

Abbildung 5: Modellhafte Darstellung der Personenidentifikatorsysteme im Ausland (Quelle: Eigene Darstellung)

Gesetzliche Grundlagen
Ein eklatanter Unterschied ist in der Anzahl der diesem System zugrunde liegenden Gesetze festzustellen (vgl. mit Abbildung 1 in Kapitel 3.4), insbesondere was die Weitergabe der Daten betrifft. Wird in den untersuchten Ländern die Erfassung, die Führung und die Verwendung der Personendaten samt Personenidentifikator aufgrund zweier Gesetze geregelt, zählt die Schweiz schon nur zwei Gesetze für die Registerführung und viele weitere für die Verwendung[10].

Infrastruktur
Während im untersuchten Ausland die Nummernvergabe durch ein zentrales Personenregister ausgeführt wird, wird der Personenstand in der Schweiz in den Zivilstandsregistern geführt und in Infostar zentralisiert. Da aber in der UPI-Datenbank dieselben Personendaten wie in Infostar registriert sind, verliert dieser Unterschied an Relevanz. Wie im untersuchten Ausland ist auch in der Schweiz diejenige Behörde für die Verwendung der Daten zuständig, die die eindeutige Nummer verwaltet.

Nutzungsberechtigte
Gemeinsam haben die Niederlande, Spanien und Dänemark, dass sie allesamt die Nutzung des eindeutigen Personenidentifikators für alle Behörden erlauben, sofern sie diese zur Erfüllung ihres gesetzlichen Auftrags benötigen. Die Nutzung durch Institutionen der Privatwirtschaft ist nur in Dänemark ohne zusätzliche Gesetzesgrundlage freigegeben, mit der Möglichkeit, dass die Betroffenen dies untersagen können.
Auch hier lässt sich ein grosser Unterschied zur Schweiz feststellen. In der Schweiz ist für jede Nutzung der AHVN13 eine separate gesetzliche Grundlage erforderlich, auch wenn die Notwendigkeit dafür bereits in einem Fachgesetz festgehalten ist.

[10] Eine abschliessende Aufzählung der Gesetze, die die systematische Nutzung der AHVN13 erlauben, konnte im Rahmen dieses Gutachtens nicht ermittelt werden. Dieses Ziel sicher zu erreichen erfordert eine Durchsicht sämtlicher Bundesgesetze und kantonalen Gesetze.

Datenschutz
In den gesetzlichen Grundlagen der untersuchten Länder wird jeweils festgehalten, dass jede Nutzung sich an die Datenschutzvorgaben zu halten hat. Hierfür verweist das entsprechende Registerführungsgesetz auf das Datenschutzgesetz. Es wird in allen untersuchten Ländern darauf geachtet, dass eine Behörde nur diejenigen Daten erhält, die sie für die Erfüllung ihres gesetzlichen Auftrages benötigt. In der Praxis findet jeweils eine Initialprüfung statt. Teilweise wird eine Vereinbarung abgeschlossen, in der der Nutzende sich zur Sicherstellung ~~Einhaltung~~ des Datenschutzes verpflichtet. Im Unterschied zur Schweiz wird die reine Verwendung eines eindeutigen Personenidentifikators nicht per se als Gefährdung des Datenschutzes wahrgenommen.

Sicherheitsbedenken
Anders als in der Schweiz wird die zweckwidrige Verknüpfung von Daten nicht als grosse Gefahr betrachtet, da jede behördliche Nutzung jeweils durch ihre entsprechenden Gesetze legitimiert ist. Diese Meinung wird auch vom Rat der digitalen Sicherheit in Dänemark, einem unabhängigen Expertenrat, der sich für Datenschutz und Datensicherheit in der digitalen Gesellschaft einsetzt, geteilt.
Sicherheitsbedenken wurden nur vom Rat der digitalen Sicherheit in Dänemark geäussert. Diese beziehen sich jedoch v.a. auf den Identitätsdiebstahl.

Empfehlungen an die Schweiz
Die befragten Experten waren sich einig, dass die Verwendung eines nationalen eindeutigen Personenidentifikators die Effizienz der Verwaltungsabläufe und die Datenqualität wesentlich erhöht. Sie sehen keine Bedenken in der Einführung eines solchen. Als konkrete Empfehlungen wurden formuliert:

- Nutzung von *privacy enhancing technologies*[11] */ privacy by design*[12]
- Physische Trennung von Identitätsdaten und anderen Daten
- Verwendung der Nummer nur zur eindeutigen *Identifikation* einer Person, nicht als Authentifizierungsmittel
- Erstellen von strengen Authentifizierungsrichtlinien
- Fördern der Nutzung von *Privacy Risk Assessments*.

Als Empfehlung wurden auch die Verwendung einer nicht-sprechenden Nummer und die Erfassung der gesamten Wohnbevölkerung erwähnt. Diese Elemente sind im AHVN13-System bereits umgesetzt.

6.2 Implikation für den Datenschutz

Die Erfahrungen im Ausland zeigen, dass die Verwendung eines nationalen, eindeutigen Personenidentifikators mit dem Datenschutz vereinbar sein kann. Die vom EDÖB skizzierten Gefahren werden im Bereich von unzulässigen Verknüpfungen von Personendatensätzen respektive der unzulässigen Bildung von Personenprofilen gesehen. Es wird regelmässig argumentiert, dass die blosse Verwendung der AHVN13 in den unterschiedlichen Registern mit Personendaten bereits per se den Datenschutz schwächt. Diese Argumentation hält einer Prüfung jedoch nicht Stand.

Das Wissen um einen Identifikator ist nicht gleich dem Zugriff auf die dahinter liegenden Daten
Die Argumentationen von Exponenten des Datenschutzes implizieren wiederholt, dass die reine Kenntnis der AHVN13 den Zugang zu den damit verknüpften respektive dahinter liegenden, schützenswerten Daten ermöglicht. Diese Schlussfolgerung ist nicht richtig. Wenn sie stimmen würde, müssten auch 1-n identifizierende Attribute automatisch den Zugang zu den restlichen, damit verbundenen Daten eines Personendatensatzes öffnen. Hier ist zwischen dem Akt der Identifikation, dem der Authentifizierung und dem der Autorisierung bezüglich Datenzugriff zu unterscheiden. Analog kann man sich vorstellen: Die private Wohnadresse einer Person ist ein Identifikator für den

[11] Ein Set von IT-Tools, IT-Applikationen und Mechanismen bzw. ein Set von IT-Massnahmen, die in Online-Dienstleistungen und IT-Fachapplikationen eingebaut werden und den Datenschutz von personenbezogenen Informationen innerhalb dieser Dienstleistungen bzw. Fachapplikationen erlauben.

[12] Ein Ansatz im Bereich Systems Engineering, der den Datenschutz im gesamten Gestaltungsprozess mitberücksichtigt.

Ort, an dem ein Teil des privaten Eigentums dieser Person liegt. Das Wissen um die private Wohnadresse ist aber weder Berechtigung zum Zugriff, noch Ermöglichung des Zugriffs auf deren privates Eigentum.
Damit nur berechtigte Personen den Zugriff auf (schützenswerte) Daten von Dritten haben, benötigt jede Datenquelle eine angemessene Lösung zur Identitäts- und Zugriffsverwaltung (oder Englisch „Identity and Access Management", IAM). Ein solches IAM für Register mit Personendaten darf nicht den eindeutigen Personenidentifikator als Attribut zur Authentifizierung eines Zugriffs auf schützenswerte Daten verwenden. Nur weil eine Person also das Wissen um den eindeutigen Personenidentifikator einer anderen Person mitbringt, darf nicht automatisch der Zugriff auf die Daten Letzterer gewährt werden.

Datenverknüpfungen finden innerhalb des rechtlichen Rahmens mit oder ohne AHVN13 statt
Die im vorliegenden Gutachten behandelten Fallbeispiele und die Erfahrungen im Ausland zeigen Datenverknüpfungen auf, die zur Erfüllung eines gesetzlichen Auftrages verlangt sind. Die Notwendigkeit einer Verknüpfung ergibt sich aus dem operativen Alltag der öffentlichen Verwaltungen, beispielsweise der Polizei, der Justiz und der Armee. In diesen Fällen sind die Verknüpfungen zwischen Personendatensätzen also rechtlich zulässig und für die Erfüllung der Aufgaben notwendig; sie sind auch ohne AHVN13 machbar und werden gemacht. Ob eine Verknüpfung von Personendaten also innerhalb oder ausserhalb des rechtlichen Rahmens stattfindet, steht daher nicht in Zusammenhang mit der Verwendbarkeit der AHVN13. Wenn eine Mitarbeiterin oder ein Mitarbeiter der Verwaltung widerrechtlich auf Personendaten in verschiedenen Registern zugreift und auf diese Weise unrechtmässig ein Profil erstellt, kann diese Person das mit oder AHVN13 tun. Warum die generelle Verwendung der AHVN13 in den Registern der öffentlichen Hand zwangsläufig oder automatisch eine Zunahme rechtswidriger Zugriffe auf Personendaten zur Folge haben sollte, ist unklar. Das Verknüpfen von Personendaten muss weiterhin (auch bei Verwendbarkeit der AHVN13) strengen, rechtlichen Auflagen unterliegen, deren Einhaltung von Seiten des Staates zu überwachen und durchzusetzen ist.
Obwohl die Datenverknüpfung erlaubt oder sogar notwendig ist, gelingt es zudem, wie aus den Fallbeispielen ersichtlich ist, wegen dem fehlenden Personenidentifikator oft nicht, die Datenverknüpfungen tatsächlich herzustellen. Dadurch entsteht Behörden oder auch Privaten ein - mittels Personenidentifikator einfach vermeidbarer - Schaden.

Die Nichtverwendbarkeit der AHVN13 schwächt den Datenschutz
Wie aus den Fallbeispielen ersichtlich, werden durch die Nichtverwendbarkeit der AHVN13 in diversen Bereichen alternative Lösungen notwendig, um Personendatensätze miteinander zu verknüpfen, abzugleichen oder zu übertragen. Aufgrund der Nichtverwendbarkeit der AHVN13 wird in einigen Fällen ein eigener Identifikator geschaffen, der auf lokalen Register- und Datennutzungsbestimmungen basierend organisationsübergreifend verwendet wird. Wo Personendatensätze zwischen Registern zu verknüpfen sind, geschieht die Identifikation der Personen über den Vergleich einer variierenden Anzahl von identifizierenden Attributen. Obschon es sich bei solchen, bereits heute stattfindenden, Verknüpfungen von Personendaten um rechtlich einwandfreie Aktionen handelt, müssen Umgehungslösungen zur Anwendung kommen, die vermeidbare Kosten verursachen und eine deutliche Gefahr von Falschidentifikation bergen. Diese Falschidentifikationen führen, wie in den Fallbeispielen beschrieben, zwangsläufig zu Verletzungen des Datenschutzes, weil Daten der falsch identifizierten Person eingesehen, verknüpft und weitergegeben werden.

Die Verwendung der AHVN13 in den Registern der öffentlichen Hand stärkt den Datenschutz
Die eingehenden Beschreibungen der Fallbeispiele und der Tabelle 1 in Kapitel 6.3. fassen die Gefahren zusammen, die sich durch das Fehlen eines eindeutigen Personenidentifikators ergeben. Durch die Verwendbarkeit der AHVN13 in Registern können Fehlidentifikationen bei legitimen Handlungen der öffentlichen Hand deutlich reduziert werden. In Fällen von zeitlicher Dringlichkeit können dezentral gespeicherte Personendatensätze schneller korrekt identifiziert werden.
Im Falle eines Identitätsdiebstahls ist dieser – ein angemessenes IAM mit entsprechendem Logging vorausgesetzt – schneller und genauer feststellbar.
Die Möglichkeit, personenbezogene Daten mit der AHVN13 zu verbinden, würde den datenführenden Behörden ausserdem die Gewährung der datenschutzrechtlichen Auskunft (Art. 8 DSG) deutlich erleichtern. Auf diese Art könnten sie einfach, schnell und vor allem vollständig offen legen, über

welche Informationen sie über die anfragende Person verfügen. Ebenso wären Datenbestände bezüglich der Nutzungsbefugnisse (wer darf welche Daten wie nutzen) viel einfacher zu prüfen, als dies heute ohne einheitlichen Personenidentifikator machbar ist. Um die Auskunftspflicht und die Kontrolle zu unterstützen, wäre die Führung eines Metadatenverzeichnisses der mit der AHVN13 verbundenen Informationen ein sehr starkes Mittel zur Durchsetzung eines umfassenden Datenschutzes.

All das stärkt den Datenschutz.

Als Antwort auf das Gutachten Biaggini (2002) kann argumentiert werden, dass das öffentliche Interesse für die Verwendung der AHVN13 als einheitlicher, organisationsübergreifender Personenidentifikator gegeben ist, da dies den Datenschutz stärken würde.

6.3 Risiken durch Nichtverwendung eines eindeutigen Personenidentifikators in der Schweiz

In diesem Kapitel werden die in den Fallbeispielen geäusserten Risiken in Zusammenhang einer Nichtverwendung der AHVN13 zusammengetragen und einer Synthese unterzogen. Tabelle 1 listet sämtliche besprochenen und bekannten Fälle auf.

Fallbeispiel	**Verwendungszweck**	**Abwicklung heute**	**Risiko im heutigen Verfahren**
VOSTRA	Leumundsprüfung im militärischen Rahmen der Rekrutierung oder Beförderung	Manuelle Identifikation mittels Personenattributen[13]	Falschidentifikation einer Person
VOSTRA	Verbesserung des rechtmässigen Informationsaustausches zwischen Behörden (u.a. bei Umgang mit Waffen)	Manueller Abgleich zwischen den föderalen Ebenen, teilweise Unterstützung durch Schnittstellen	Falschidentifikation einer Person
VOSTRA	Prüfung Straffälligkeit bei Einbürgerungen	Einzelabfragen im VOSTRA	Falschidentifikation einer Person
VOSTRA	Individuelle Strafregisterauszüge	Einzelabfragen im VOSTRA	Übergabe eines falschen Auszugs aufgrund Falschidentifizierung und damit Verletzung des Datenschutzes durch Bekanntgabe von vertraulichen Informationen einer anderen Person
Mehrwertsteuerunterstellung	Risikoprüfung d.h. Prüfung, ob die Person in Zusammenhang mit anderen Firmen noch offene MwSt-Posten hat	Manuelle Abklärungen durch eine(n) Sachbearbeiter/-in	Risiko nicht ermittelt; offene Posten bleiben, ohne Konsequenzen für Schuldner, offen.
Rückerstattung der Verrechnungssteuer von ausländischen Staatsangehörigen	Risikoprüfung d.h. Ermittlung offener Posten vor Auszahlung	Manuelle Abklärungen durch eine(n) Sachbearbeiter/-in	Risiko nicht ermittelt; Betrag wird trotz möglicher offener Posten ausbezahlt.

[13] Familienname, Geburtsname, Vorname(n), Geburtsdatum, Namen und Geburtsdatum der Eltern

Fallbeispiel	Verwendungszweck	Abwicklung heute	Risiko im heutigen Verfahren
Asa	Verwaltung Lehrpersonal für angebotene Ausbildungskurse	Verwendung der FABER ID für Personen mit Führerausweis Verwendung AHVN13 für Personen ohne Führerausweis notwendig	Keine Identifikation von Lehrpersonal ohne Führerausweis möglich.
Asa	Identifizierung von Ärztinnen und Ärzten ohne Führerausweis bei obligatorischen Weiterbildungen	Verwendung der FABER ID für Personen mit Führerausweis Verwendung der GLN für Personen ohne Führerausweis	Kein Risiko; wegen mehrerer Identifikatoren allerdings Zusatzkosten.
Strassenverkehrsämter	Kommunikation zwischen StVA der Kantone und den Einwohnerkontrollen	Manuelle Verarbeitung	Versenden Kfz-Steuern an falsche Adressen
Strassenverkehrsämter	Eindeutiger Identifikator für die Halterinnen und Haltern von Schiffen	Jeder Kanton vergibt einen eigenen Identifikator	Im Falle eines Unfalls ist die Ermittlung der Halterschaft aufwändig bis unmöglich.
VOSTRA	Sonderprivatauszug (Pädophilenregister)	Manuelle Identifikation mittels mehrerer Attribute	Falschidentifikation, Beschuldigung falscher Person mit existenzbedrohenden Konsequenzen
Betreibungsregister (kommunal, Stadtkreise)	Betreibungsauszug	Manuelle Identifikation mittels mehrerer Attribute	Falschidentifikation, Erschleichung fremder Betreibungsauszüge
Betreibungsregister (kommunal, Stadtkreise)	Betreibungsbegehren	Manuelle Identifikation mittels mehrerer Attribute	Falschidentifikation, Belästigung von Unbeteiligten mit einer Betreibung
Handelsregister (kommunal, Stadtkreise)	Handelsregisterauszug bei Strafsachen	Manuelle Identifikation mittels mehrerer Attribute	Falschidentifikation
Grundbuch	Sperrung von Vermögen	Manuelle Identifikation mittels mehrerer Attribute	Falschidentifikation, Sperrung von Vermögen falscher Personen; Nichtauffindbarkeit von Vermögen im Erb- oder Straffall

Tabelle 1: Risiken in heutigen Verfahren

Die Liste in Tabelle 1 zählt 15 Fallbeispiele auf. In drei Fällen ist bereits ein Personenidentifikator im Einsatz. In allen anderen Fällen erfolgt die Identifikation der Personen manuell.

In allen Fällen werden Behörden in der Erfüllung ihres gesetzlichen Auftrags stark behindert. In neun Fällen zieht die Nichtverwendung der AHVN13 ein Risiko für Falschidentifikation nach sich. Dieses Risiko kann bedeutende Konsequenzen für die betroffenen Personen haben. So können Datenschutzverletzungen aber auch Falschbeschuldigungen die Folge sein. In vier Fällen ist die Identifikation ohne Verwendung eines Personenidentifikators kaum möglich. Der Staat bleibt in diesen Fällen teilweise in Unwissenheit. Diese Fälle kommen v.a. in Zusammenhang mit der Ermittlung von Vermögenswerten vor.

In den Fällen, in denen ein Personenidentifikator bereits zum Einsatz kommt, bestehen weiterhin Probleme in der Identifikation von Personen. So wird die FABER ID nur an Personen mit Führerausweis vergeben. Die Verwaltungsabläufe, die die FABER ID als Personenidentifikator nutzen, stossen an Grenzen, sobald sie

- Personen ohne Führerausweis in ihrem System erfassen müssen;
- Informationen von Behörden benötigen, die die FABER ID nicht führen.

6.4 Kostenschätzung

Die Einschätzung der Kosten gestaltete sich als schwieriges Unterfangen mit vielen Unbekannten. Die aktuellen Aufwände in den jeweiligen Bereichen lassen keine klare Zuordnung der für die Identifikationsarbeit anfallenden Kosten zu. Einerseits, weil sie mit anderen Aufwänden zusammengefasst erscheinen oder weil sie faktisch nicht existent sind, da eine Identifikation im heutigen System kaum möglich ist. Auch die Einschätzung der zukünftigen Kosten gestaltet sich schwierig, weil diese je nach Ausgangslage stark variieren kann. Dieses Kapitel liefert deshalb lediglich einen möglichen Ansatz für eine Kostenbetrachtung.

Kosteneinschätzung aus Sicht einer Behörde
Die Kosten ergeben sich auf Ebene der notwendigen Systeme (Konzeption, Implementierung, Betrieb, Pflege), der Daten (Erfassung, Abgleich, Pflege), der Prozesse (Identifikation, Abgleich, Zusammenführung) und der Gesetzgebung.

Für eine gesamthafte Kostenanalyse wird von einem IST-Zustand ausgegangen. Diese Kosten setzen sich aus Compliance Anforderungen (Gesetze), den Prozesskosten (u.a. Identifikation von Personen, Prozesslaufzeit), Datenverwaltung, (u.a. Erfassung und Pflege der Daten) und den aktuell im Einsatz stehenden IT-Infrastrukturen (Betrieb, Support) zusammen. Bei einer geplanten Einführung der AHVN13 als eindeutiger Personenidentifikator sind mit entsprechenden Kosten für die Anpassung der Systeme und Prozesse zu rechnen. Hier fallen Kosten für die Anpassung der Prozesse, Daten (Migrationen, Abgleich, Zusammenführung), notwendige Anpassung IT-Infrastruktur (Konzeption, Implementierung) und Gesetzgebung an. Ziel einer solchen Umstellung muss sein, dass die Kosten im SOLL-Betrieb tiefer sind als im IST-Zustand und damit die Migrationskosten über die Zeit eingespart werden können.

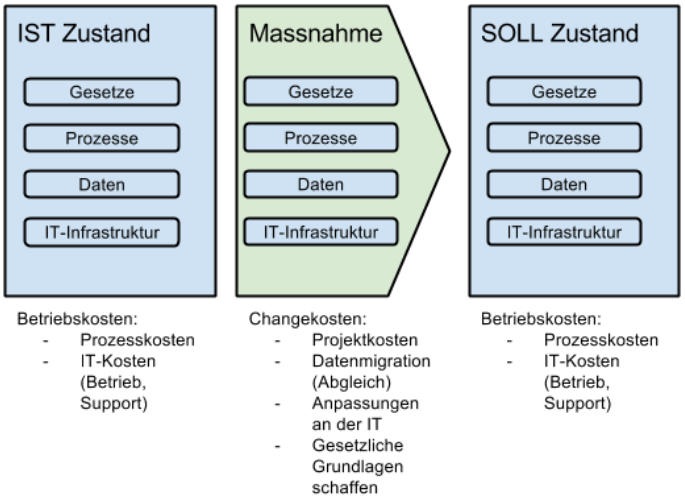

Abbildung 6: Analyse der Kosten aus Behördensicht

Der im Kapitel 4.6 beschriebene Strafregisterfall von VOSTRA geht von einer provisorischen Kostenschätzung für die Einführung der AHVN13 und Anpassungen am System von ca. 1,9 Millionen CHF aus. Für die laufenden Kosten wird ein Aufwand von ca. 400‘000 CHF Personalkosten geschätzt. Weitere Kostenschätzungen sind nicht bekannt.

Kosten aus gesamtwirtschaftlicher Perspektive
Bei der Einführung eines Personenidentifikators kann von drei Arten von Lösungen ausgegangen werden:

1. Register, welche die AHVN13 als Identifikator führen dürfen (Direkte Nutzung der AHVN13: Typ A)
2. Register, welche Identifikatoren von der AHVN13 ableiten und sektoriell verwenden dürfen (Indirekte Nutzung der AHVN13: Typ B)
3. Register, welche eigene Identifikatoren führen, die in keinem Zusammenhang mit der AHVN13 stehen (Nichtverwendung der AHVN13: Typ C)

Welche Kosten aus gesamtschweizerischer Sicht jeweils entstehen, ist in Tabelle 2 dargestellt.

Gesamtschweizerisch, auf wenige Sektoren reduziert, führt heute jedes Register seine eigenen Identifikatoren für sich (vgl. Typ C in Tabelle 2). Register, welche nicht auf die AHVN13 als eindeutiger Personenidentifikator zurückgreifen können oder davon abgeleitete Identifikatoren benützen dürfen, müssen eigene Lösungen für Personenidentifikatoren konzipieren, implementieren, betreiben und pflegen (vgl. Typ B und C in Tabelle 2). In der Regel bedeutet dies auch, dass sie Personenidentifikationsdaten erheben und pflegen müssen. Die Prozesse dazu sind erfahrungsgemäss aufwändig, schwierig zu beherrschen und fehleranfällig, was sie entsprechend kostenintensiv macht. Wie dies aus den Fallbeispielen ersichtlich ist, ist diese Situation aktuell die Norm und kommt auf allen föderalen Ebenen der Schweiz vor.

Register, welche auf die AHVN13 als eindeutiger Personenidentifikator zurückgreifen dürfen, benötigen dazu eine gesetzliche Grundlage (vgl. Typ A in Tabelle 2). Diese ist für jeden Anwendungsfall einzeln zu schaffen, sowohl auf Ebene des Bundes, wie auch auf Ebene jedes einzelnen Kantons. Die konkreten Kosten für eine Gesetzgebung auf den föderalen Ebenen der Schweiz sind derzeit nicht bekannt, dürften aber nach Auskunft von Experten jeweils „in Personenjahren“ anfallen, also gegen 1 Mio CHF je Gesetz zu liegen kommen.

Ohne Verwendung eines Personenidentifikators entstehen täglich Kosten als Folge der Laufzeitprozesse zur Identifikation wie auch zum Abgleich und zur Zusammenführung.

- Identifikation: Personendaten in den unterschiedlichen Registern müssen den korrekten Personen zugeordnet werden können. Wo die jeweiligen Identifikatoren gegen aussen nicht bekannt sind (was bei Registern mit unabhängigen Identifikatoren die Norm ist), muss die reale Person zum angefragten Datensatz auf Basis von 1-n Personenidentifikationsattributen abgeglichen werden. In vielen Fällen ist ein manueller Prozess notwendig (vgl. Fallbeispiele, z.B. weil die Namensschreibweise nicht stimmt). Diese Identifikationsprozesse geschehen tausendfach jeden Tag in der Schweiz. Während die Prozessausführung (insbesondere im manuellen Fall) personalintensiv und entsprechend kostspielig ist, sind die Folgen von Fehlidentifikationen (die insbesondere bei manuellen Prozessen unvermeidbar sind) zum Teil gravierend und verursachen durch nachgelagerte Prozesse weitere Kosten.
- Abgleich & Zusammenführung: Die Personendatensätze in den verschiedenen Registern müssen regelmässig miteinander abgeglichen werden, teilweise sind auch Über- oder Zusammenführungen in andere Register notwendig. Auch hier tritt das Problem der Identifikation zu Tage. Die Folge sind wiederum kostenintensive Abgleichprozesse, mitunter ebenfalls auf manuellem Weg. Wo Personendaten initial mit mangelnder Qualität von einem Register in ein anderes übertragen wurden, werden in der Folge kostenintensive Bereinigungsprozesse notwendig. Auch diese Kosten fallen in der Schweiz tausende Male pro Jahr an.

Tabelle 2 zeigt, dass die Zahl der Aufwände bei einer Nichtverwendung der AHVN13 höher ist als bei deren Verwendung. Obwohl die tatsächliche Kostenhöhe jeweils von der Anzahl Transaktionen und der im jeweiligen Register geführten Datenmenge (z.B. nur Fahrzeughaltende, statt die gesamte Wohnbevölkerung der Schweiz) abhängig ist, gilt es zu berücksichtigen, dass die in Tabelle 2 aufgezeigten Gesamtkosten jeweils mehrmals anfallen. Diese Kosten werden bei jeder neuen direkten oder indirekten Verwendung der AHVN13 generiert, und jedes Mal, wenn in einem Sektor ein von der AHVN13 unabhängiger Personenidentifikator aufgebaut wird. Insofern sind die in Tabelle 2 aufgezählten Gesamtkosten mit der Anzahl Verwendungen / Anzahl Sektoren zu multiplizieren. Während im Falle abgeleiteter Lösungen (Typ B) noch grosse Mengen an Personen in gemeinsamen Systemen erfasst und die Daten gepflegt werden, so fallen die entsprechenden Aufwände im dritten Falle (Typ C) zig-fach an. In Anbetracht der Tatsache, dass in der Schweiz aktuell Typ C vorherrschend ist, kann festgehalten werden, dass die Schweiz zurzeit die kostspieligste Lösung praktiziert.

Anfallende Kosten / Aufwände	Kostenart	Anfallende Kosten Direkte Nutzung (Typ A)	Anfallende Kosten indirekte Nutzung (Typ B)	Anfallende Kosten Nichtverwendung (Typ C)
Erstellung einer gesetzlichen Grundlage	Kosten Systemeinführung	√	√	
Erstellung eines Personenregisters für Nummernvergabe				√
Datenbereinigung / -migration (Abgleich)		√	√	√
IT-Anpassungen bei beteiligten Registern		√	√	√
Zustellung der neuen Nummer an die Nummerninhaber/-innen			√	√
Laufende IT-Kosten für den Betrieb des Personen- bzw. Nummernregisters	Kosten laufender Betrieb		√	√
Laufende Nummernzuordnung (Neuerfassung von Daten)			√	√
Sicherung der Qualität und Aktualität bestehender Daten (Datenmutation bei Namensänderungen etc.)			√	(√)[14]
Bei den beteiligen Registern anfallende Kosten für den laufenden Abgleich der Daten mit dem Nummernregister		√	(√)[15]	(√)[16]
Kosten gesamthaft		Bei jeder neuen systematischen Verwendung fallen Kosten für die Erstellung einer gesetzlichen Grundlage und für die Anbindung an das bestehende System an.	Die Kosten für den Aufbau und die Führung eines Nummernregisters fallen weg. Trotzdem fallen Kosten für die Vergabe und die Pflege der sektoriellen, abgeleiteten Nummern bei jeder neuen Verwendung an.	Die Erstellung von unabhängigen Identifikatoren erfordert eine am Fach angepasste Replikation des AHVN13-Systems. Die Höhe der Kosten ist abhängig von der im replizierten System geführten Datenmenge und Anzahl Transaktionen.

Tabelle 2: Kosten aus gesamtwirtschaftlicher Sicht

[14] Zur Kostenreduktion wird oft auf die Sicherung der Aktualität und der Qualität der im Register geführten Daten verzichtet.

[15] Ob diese Kosten anfallen oder nicht ist abhängig von der Art der Nutzung der Nummer.

[16] Bei Registern, die nicht mit anderen Registern verknüpft sind, fallen diese Kosten weg.

Abschliessend kann festgestellt werden, dass diese schweizweit konstant anfallenden Kosten bis dato nicht erhoben werden. Üblicherweise hören die Kostenrechnungen (etwa bei Regulierungsfolgeabschätzungen) bei den initialen Aufwänden und den Betriebsaufwänden für die Personenidentifikationssysteme auf. Die durch das Fehlen eines Personenidentifikators anfallenden, wiederkehrenden und grösstenteils vermeidbaren Kosten, bleiben bislang versteckt. Über die Kosten der Spezialgesetze zur Verwendung der AHVN13 auf Ebene Bund und der 26 Kantone herrscht ebenfalls keine Transparenz. Nimmt man die bekannten Kosten von Einführung und Betrieb der UPI als Basis, so dürften bei schweizweiter, genereller Verwendbarkeit der AHVN13 in öffentlichen Registern die potentiellen Kosteneinsparungen wahrscheinlich jährlich im dreistelligen Millionenbereich jährlich zu liegen kommen.

7 Schlussfolgerung

Die Schweiz verfügt bereits über einen nationalen, eindeutigen Personenidentifikator
Wie in Kapitel 6.1. dargestellt, ist die heute existierende Infrastruktur rund um die AHVN13 mit der Infrastruktur in den nationalen Personenidentifikatorensystemen im untersuchten Ausland vergleichbar. Das System in der Schweiz ist gar als fortschrittlich einzustufen, weil es eine Nummer führt, die keine Rückschlüsse auf die nummerinhabende Person zulässt, und die gesamte Wohnbevölkerung ab Geburt oder Zuzug erfasst wird.

Die Schweiz braucht einen einheitlichen, organisationsübergreifenden Personenidentifikator
Kapitel 6.3_Risiken_durch_Nichtverwendung zeigt auf, dass das Fehlen eines eindeutigen Personenidentifikators Verwaltungsabläufe nicht nur massiv erschwert, sondern auch beachtliche Risiken nach sich zieht. Behörden werden in der Ausführung ihrer Aufgaben dadurch teilweise stark behindert, unbetroffene Personen potentiell geschädigt.

Der Einsatz des bereits bestehenden nationalen eindeutigen Personenidentifikators AHVN13 ist unbedingt zu erwägen. Allein die Zahl der Fälle, die im Rahmen dieses Gutachtens erhoben wurden, deutet darauf hin, dass der Bedarf nach einem eindeutigen Personenidentifikator ein allgemeines Bedürfnis ist. Zudem stösst der Einsatz eines sektoriellen Personenidentifikators schnell an Grenzen.

Die beschriebenen Fallbeispiele illustrieren, dass das Fehlen eines eindeutigen Personenidentifikators fallweise auch Datenschutzverletzungen zur Folge haben. Damit ist das im Gutachten Biaggini (2002) geforderte Öffentlichkeitsinteresse nicht nur durch Forderungen nach einer erhöhten Datenqualität und Effizienzsteigerungen zu bewerten, sondern auch durch das allgemeine Bedürfnis, die Risiken, die die aktuelle Situation (auch bezüglich Datenschutz) birgt, zu beheben.

Die gesamthafte Betrachtung der Fallbeispiele zeigt auch auf, dass die einzige Alternative zur Verwendung der AHVN13 in der Schaffung eines sektoriellen Personenidentifikators liegt. Wie die Fallbeispiele aus dem Verkehrsbereich jedoch zeigen, stossen Systeme mit sektoriellen Personenidentifikatoren rasch an Grenzen. Mangels einer Alternative streben einzelne Behörden nun die Schaffung der gesetzlichen Grundlagen an, um die AHVN13 systematisch zu verwenden. Damit ist auch der im Gutachten Biaggini (2002) geforderte Erforderlichkeitsnachweis erbracht.

Die Verwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators ist mit dem Datenschutz vereinbar
Die in der Schweiz geführte Diskussion unterscheidet nicht zwischen Identifikation, Authentifizierung und Autorisierung. Ein eindeutiger Personenidentifikator dient der eindeutigen Identifikation einer Person, mangels anderer eindeutigen Personenmerkmale. Wie alle anderen Personendaten sollte der Personenidentifikator lediglich als weiteres Merkmal betrachtet werden, das es zu schützen gilt. Einzigartig an diesem Personenmerkmal ist, dass es vom Staat vergeben wird.

Die Daten gilt es in digitalen Abläufen mit einem adäquaten Identitäts- und Berechtigungsverwaltungssystem und durch den Einsatz von *privacy enhancing technologies* zu

sichern. Weiter zeigen die Erfahrungen im Ausland, dass *Privacy Risk Assessments* ein gutes Mittel sind, um den Datenschutz in Verwaltungsabläufen zu sichern. *Privacy Risk Assesments* enthalten Empfehlungen, wie eine IT-Infrastruktur und die Prozesse rund um eine bestimmte Datenverknüpfung ausgestaltet sein sollten, um den Datenschutzvorgaben zu genügen. Die Berechtigung auf Datenzugang muss klar geregelt sein und darf sich nicht allein auf die als eindeutigen Personenidentifikator verwendete Nummer stützen. Abschliessend ist zu bemerken, dass diese Schutzmassnahmen auch ohne Verwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators notwendig sind.

Werden die vorangehend erwähnten Sicherheitsmassnahmen angewendet, stärkt die Verwendung eines einheitlichen, organisationsübergreifenden Personenidentifikators sogar den Datenschutz. Wie aus den Fallbeispielen ersichtlich, könnten heute vorkommende Datenschutzverletzungen verhindert werden, und es wäre einer Behörde ein Leichtes, einer Person Auskunft zu den über sie gehaltenen und verarbeiteten Daten zu geben.

Die heutige Situation ist nicht zufriedenstellend
Die aufgezählten Risiken und die hohen jährlichen Kosten drängen auf eine schnelle Lösung, die es ganzheitlich statt einzeln anzugehen gilt. Obwohl zahlreiche Bereiche vor demselben Problem stehen, muss heute für jedes Problem die Lösung einzeln geschaffen werden. Für die Schweiz insgesamt entstehen damit jedes Mal Kosten für die Schaffung einer Gesetzesgrundlage, und allenfalls Kosten für die Schaffung eines Personenregisters, das die Vergabe und Pflege eines Identifikators für einen Teil der Bevölkerung (z.B. Personen mit Führerausweis) ausführt.

Für die Schweiz würde es sich lohnen, die AHVN13 als nationalen, eindeutigen Personenidentifikator in staatlichen Verwaltungen zu verwenden, zumal sie bereits eine entsprechende Infrastruktur betreibt und der Bedarf nach einem Personenidentifikator in zahlreichen Bereichen vorhanden ist. Wird die Verwendung der AHVN13 als nationaler, eindeutiger Personenidentifikator erwogen, ist es jedoch nicht hinreichend, die gesetzliche Grundlage dahingehend zu ändern. Es muss ein Gesamtsystem konzipiert werden, das die Gefahren im Hinblick auf den Datenschutz von Anfang an ernst nimmt und in die gesetzliche, technische und organisatorische Ausgestaltung integriert.

Mit Blick auf internationale Verpflichtungen der Schweiz sind die Kriterien dieser Nummer international zu vereinbaren. Im Rahmen des automatischen Informationsaustausches ist nicht nur die Identifikation von in der Schweiz wohnhaften Personen von Bedeutung. Die Identifikation von nicht in der Schweiz wohnhaften ausländischen Staatsangehörigen ist hier ebenso von Relevanz. Umgekehrt ist es auch für ausländische Behörden von Relevanz, im Rahmen dieser Vereinbarung schweizerische Staatsangehörige mittels einer eindeutigen Nummer identifizieren zu können.

8 Empfehlungen

Der Schweiz wird angeraten, die in diesem Gutachten beschriebenen Probleme ganzheitlich anzugehen. Es wird empfohlen, ein Konzept für ein Gesamtsystem „nationaler eindeutiger Personenidentifikator“ zu erstellen, das den Schutz von Personendaten ins Zentrum stellt, das bestehende System der AHVN13 mitberücksichtigt und die legalen, technischen und organisatorischen Betrachtungen enthält.

Weiter wird der Einbezug der Datenschutzbehörde bereits in der Initialisierungsphase (gemäss Hermes 5.1) empfohlen. Die Aktivitäten sind auch mit den aktuell laufenden nationalen Projekten zur Einführung eines nationalen elektronischen Identitätsnachweises (eID) [26] und dem Aufbau eines Identitätsverbundes Schweiz (IDV) [27] zu koordinieren. Die Entwicklungen im Zusammenhang mit dem Postulat 12.3361 der Staatspolitischen Kommission des Nationalrats zum Thema Adressdatenaustausch zwischen Einwohnerregistern, Post und anderen Dateninhabern sind mit zu verfolgen [28].

Die Entwicklungen und Anforderungen im internationalen Kontext sind zu berücksichtigen.

9 Abbildungsverzeichnis

10 Tabellenverzeichnis

11 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AHV	Alters- und Hinterlassenenversicherung
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
AHVN13	13-stellige AHV-Versichertennummer
Asa	Verkehrsvereinigung der Strassenverkehrsämter
ASTRA	Bundesamt für Strassen
BAG	Bundesamt für Gesundheit
BFH	Berner Fachhochschule
BFS	Bundesamt für Statistik
BJ	Bundesamt für Justiz
BRP	Personenbasisregister (Basisregistratie personen)
BSN	Bürgerservicenummer (Citizen Service Number)
BSV	Bundesamt für Sozialversicherungen
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
CPR	Det Centrale Personenregister
DNI	Nummer der Identitätskarte (Documento Nacional de Identidad)
EDÖB	Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter
EFK	Eidgenössischen Finanzkontrolle
ESTV	Eidgenössische Steuerverwaltung
FABER	Fahrberechtigungsregister
GLN	Global Location Number, ehemals EAN

Infostar	Eidgenössischer Zivilstandsregister
ISC-EJPD	Informatik Service Center des Eidg. Justiz- und Polizeidepartement
KfZ	Kraftfahrzeug
MwSt	Mehrwertsteuer
NIF	Steuernummer (Número de Identificación Fiscal)
PISA	Personalinformationssystem der Armee
RHG	Registerharmonisierungsgesetz
SARI	System für Administration, Registrierung und Information
SIK	Schweizerische Informatikkonferenz
SoFi number	Sozialversicherungs- und Steuernummer in den Niederlanden
StVA	Strassenverkehrsamt
UID	Unternehmens-Identifikationsnummer
UPI	Unique Person Identification
VOSTRA	Vollautomatisiertes Strafregister
VVK	Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung
ZAS	Zentrale Ausgleichsstelle
ZEMIS	Ausländer- und Asylbewerberregister

12 Literaturverzeichnis

[1] Zentrale Ausgleichsstele ZAS, «AHVN13. Die 13-stellige AHV-Nummer (AHVN13) im Bereich der Sozialversicherungen des Bundes,» [Online]. Available: http://www.zas.admin.ch/org/00721/00722/index.html?lang=de. [Zugriff am 19 06 2015].

[2] Zentrale Ausgleichsstelle ZAS, «UPI,» [Online]. Available: http://www.zas.admin.ch/org/00721/00758/index.html?lang=de. [Zugriff am 19 06 2015].

[3] Zentrale Ausgleichsstelle ZAS (NAH/REY), «UPI - Benutzerhandbuch (handbook). Version 1.04,» 21 November 2012. [Online]. Available: http://www.zas.admin.ch/org/00721/00758/00904/index.html?lang=de. [Zugriff am 19 06 2015].

[4] Bundesamt für Sozialversicherungen BSV, «Verwendung AHVN13 Pflichtenheft. Version 1.2,» 21 November 2012. [Online]. Available: http://www.zas.admin.ch/org/00721/00722/00896/index.html?lang=de. [Zugriff am 19 06 2015].

[5] Bundesamt für Statistik BFS, «Harmonisierung amtlicher Personenregister. Amtlicher Katalog der Merkmale.,» 2014. [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.html?publicationID=5567. [Zugriff am 19 06 2015].

[6] Zentrale Ausgleichsstelle ZAS, «Verzeichnis der systematischen Benutzer der AHVN13,» 16 April 2015. [Online]. Available: http://www.zas.admin.ch/org/00721/00722/00901/index.html?lang=de. [Zugriff am 19 06 2015].

[7] Der Schweizerische Bundesrat, «Verordnung über die Versichtertenkarte für die obligatorische Krankenpflegeversicherung (VVK),» 1 Januar 2009. [Online]. Available:

https://www.admin.ch/opc/de/classified-compilation/20062093/200901010000/832.105.pdf. [Zugriff am 01 06 2015].

[8] G. Biaggini, «Ein Personenidentifkator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV). Rechtsgutachten.,» [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/00949/index.html?lang=de. [Zugriff am 26 06 2015].

[9] Eidgenösssicher Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), «AHV-Nummer,» [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/index.html?lang=de. [Zugriff am 26 06 2015].

[10] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, «Keine weitere Verbreitung der AHV-Versichternnummer,» 16 April 2014. [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/index.html?lang=de. [Zugriff am 30 06 2015].

[11] Eidgenössische Steuerverwaltung ESTV, «Die Hauptabteilung Mehrwertsteuer,» [Online]. Available: http://www.estv.admin.ch/mwst/org/00338/00344/00353/index.html?lang=de. [Zugriff am 30 06 2015].

[12] Eidgenössische Finanzkontrolle EFK, «11391 ESTV Organisation und Instrumente der Betrugserkennung und Betrugsbekämpfung im Bereich Mehrwertsteuer».

[13] Bundesamt für Justiz BJ, «Merkmale des Grundbuchs,» [Online]. Available: https://www.bj.admin.ch/bj/de/home/wirtschaft/grundbuch/merkmale.html. [Zugriff am 25 06 2015].

[14] Bundesamt für Justiz BJ, «Datenmodelle eGris,» [Online]. Available: https://www.bj.admin.ch/bj/de/home/wirtschaft/grundbuch/datenmodelle.html. [Zugriff am 02 07 2015].

[15] Der Schweizerische Bundesrat, «Botschaft zur Änderung des Schweizerischen Zivilgesetzbuches (Beurkundung des Personenstands und Grundbuch) vom 16. April 2014,» 16 April 2014. [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2014/3551.pdf. [Zugriff am 25 06 2015].

[16] Der Schweizerische Bundesrat, «Verordnung über das Fahrberechtigungsregister,» 1 Oktober 2011. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20001349/index.html. [Zugriff am 22 Juni 2015].

[17] Der Schweizerische Bundesrat, «311 Verordnung über das Strafregister (VOSTRA-Verordnung),» 01 Januar 2015. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20061863/index.html. [Zugriff am 06 2015].

[18] Der Schweizerische Bundesrat, «Botschaft zum Bundesgesetz über Verbesserungen beim Informationsaustausch zwischen Behörden im Umgang mit Waffen - 13.109,» 13 Dezember 2013. [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2014/303.pdf. [Zugriff am 06 2015].

[19] Social Security Administration (GlobalDenmark Translations), «Executive Order on the Civil Registration System Act,» Juli 2013. [Online]. Available: https://cpr.dk/media/163624/lovbekendtg_relse_eng_12070213.pdf. [Zugriff am 15 06 2015].

[20] The Danish Data Protection Agency, «Compiled version of the Act on Processing of Personal Data,» December 2012. [Online]. Available: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/. [Zugriff am 15 06 2015].

[21] Rådet for Digital Sikkerhed, «Digital sikkerhed i Danmark 2014. Årsrapport fra Rådet for Digital Sikkerhed.,» März 2015. [Online]. Available: http://digitalsikkerhed.dk/nyheder/nyhederfraraadet/nyhed/article/419/. [Zugriff am 15 06 2015].

[22] Government of the Netherlands, «Identification documents. The Citizen Service Number (BSN),» [Online]. Available: http://www.government.nl/issues/identification-documents/the-citizen-service-number. [Zugriff am 24 06 2015].

[23] Government of Netherlands, «Identification documents. The Municipal Personal Records

Database,» [Online]. Available: http://www.government.nl/issues/identification-documents/the-municipal-personal-records-database. [Zugriff am 24 06 2015].

[24] Rijksdienst voor Identiteisgegevens. Ministerie van Binnenlandse Zaken en Koningkrijksrelaties., «BSN,» [Online]. Available: http://www.rijksdienstvooridentiteitsgegevens.nl/BSN/Vraag_en_antwoord/Wetgeving. [Zugriff am 24 06 2015].

[25] MINISTERIO DEL INTERIOR. Dirección General de la Policía., «Descripción del DNI electrónico,» [Online]. Available: http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_103&id_menu=[1]. [Zugriff am 24 06 2015].

[26] Bundesamt für Justiz BJ, «Informelle Konsultation elektronischer Identitätsnachweis,» 08 07 2015. [Online]. Available: https://www.fedpol.admin.ch/fedpol/de/home/pass---identitaetskarte/pass_idk/ausweise.html. [Zugriff am 04 08 2015].

[27] E-Government Schweiz, «B2.06 Dienst für die Identifikation und Berechtigungsverwaltung. Vertrauenswürdige Identitäten über Organisationsgrenzen hinweg.,» [Online]. Available: http://www.egovernment.ch/b206/index.html?lang=en. [Zugriff am 04 08 2015].

[28] Der Schhweizerische Bundesrat, «Adressdatenaustausch zwischen Einwohnerregistern, Post und anderen Dateninhabern. Bericht des Bundesrates in Erfüllung des Postulats 12.3661 der Staatspolitischen Kommission des Nationalrats vom 16. August 2012,» 12 November 2014. [Online]. Available: http://www.parlament.ch/sites/doc/CuriaFolgeseite/2012/20123661/Bericht%20BR%20D.pdf. [Zugriff am 04 08 2015].

[29] Der Schweizerische Bundesrat, «Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenversicherung (Neue AHV-Versichertennummer),» 23 11 2005. [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2006/501.pdf. [Zugriff am 04 08 2015].

[30] Schweizerische Bundeskanzlei, «https://www.ch.ch/de/heiraten-namenswahl/,» 2015. [Online]. Available: https://www.ch.ch/de/heiraten-namenswahl/. [Zugriff am 06 2015].

[31] P. Kummer, «Rapport final. Projet "Numéro d'assuré (NAVS13) comme identificateur de personne". Harmonisation des registres.,» Office fédéral de la statistique OFS, Neuchâtel, 2010.

Anhang 1: Liste der interviewten Personen

Liste der interviewten Personen

Patrick Riesen, Eidgenössische Steuerverwaltung ESTV, Programmleiter Fiscal-IT

Urs Paul Holenstein, Bundesamt für Justiz BJ, Leiter Fachbereich Rechtsinformatik

Christian Buetler, Bundesamt für Justiz BJ, Umsetzungsprojektmanager E-Government

Sven Britschgi, Vereinigung der Strassenverkehrsämter asa, Geschäftsführer

Christine Madl, Bundesamt für Justiz BJ, Anwendungsverantwortliche VOSTRA und IT-Projektleiterin

Carsten Grage, Danish Ministry of Interior, CPR Office, Head of Division

Rasmus Theede, Danish independent Council of Digital Security, Chairman

Uijl Kees, Ministry of the Interior and Kingdom Relations, Citizenship and Information Directorate, Department of Identity, Policy Advisor

Carlos Gómez Muñoz, Ministry of Finance and Public Administration, ICT Civil Servant

Liste der konsultierten Personen

Thomas Steimer, Bundesamt für Justiz BJ, Umsetzungsprojektmanager (Experte infostar)

Jérôme Magnin, Zentrale Ausgleichsstelle ZAS, Sektionschef Statistik und Zentralregister

Patrick Kummer, Bundesamt für Statistik BFS, Abteilung Register, Sektionschef Gebäude und Wohnungen

Anhang 2: Interviewleitfaden Fallbeispiele

Einleitung

In der Schweiz gibt es keinen einheitlichen, organisationsübergreifend genutzten Personenidentifikator. Die Nutzung des verbreitetsten Identifikators, der AHVN13, erfordert eine gesetzliche Grundlage für jeden Nutzenden. Daraus ergeben sich operative Herausforderungen und Gefahren durch mangelnde Eindeutigkeit bei der organisationsübergreifenden Datenverarbeitung. Die Einführung einheitlicher, organisationsübergreifender Personenidentifikatoren wurde bis dato durch Datenschutzbedenken verhindert. Die Diskussion um den Datenschutz verhindert bessere Lösungen und ignoriert, dass auch in der Nichtverwendung der AHV-Nummer grosse Gefahren und verpasste Chancen liegen.

Die Berner Fachhochschule BFH hat von der Schweizerischen Informatikkonferenz SIK den Auftrag zur Erstellung eines Gutachtens zum Thema AHVN13 als einheitlichen, organisationsübergreifenden Personenidentifikator erhalten. Das Gutachten geht u.a. der Frage nach: „Was riskieren wir und was kostet es, solange wir auf die Verwendung eines einheitlichen, organisationsübergreifenden Identifikators verzichten?“. Mittels Interviews werden Probleme, die schon bisher aus dem Nichtgebrauch eines einheitlichen, organisationsübergreifenden Identifikators entstanden sind, erhoben. Ebenso wird bei heutigen Einsatzgebieten, in welchen ein einheitlicher, organisationsübergreifender Identifikator bereits eingesetzt wird, nach dem Nutzen gefragt.

Die Interviews zeigen die Perspektive der Organisation auf, sind aber nicht repräsentativ, sondern sind eine Aussage einer Person.

Interviewfragen

Einstiegsfrage: Was ist in Ihrem Tätigkeitsbereich der Hauptbedarf an Identifikation von Personen? Wie wird dies aktuell gemacht?

1. Kennen Sie konkrete Beispiele, die einen Schaden /Aufwand verursacht haben, weil eine Person nicht richtig identifiziert wurde?
2. Kennen Sie Anwendungsfälle oder Beispiele von Abläufen / Anwendungen, die durch die fehlende Verfügbarkeit eines eineindeutigen Personenidentifikators nicht realisierbar sind?
3. Wie oft treten solche Fälle aus den ersten beiden Fragen auf? (pro Jahr, in Ihrem Kanton, in der Schweiz)
4. Können Sie uns die daraus entstandenen finanziellen und nicht-finanziellen Folgen schildern?

5. In welchen Fällen werden Daten verknüpft und in welchen dieser Fälle wäre die Verwendung der AHVN13 als einheitlicher, organisationsübergreifender Personenidentifikator sinnvoll?
6. Wie werden die Personendaten heute verknüpft und welche Probleme treten dabei auf?

7. Welcher Aufwand und welche Kosten könnten durch die Verwendung der AHVN13 als einheitlichen, organisationsübergreifenden Personenidentifikator insgesamt eingespart werden?
8. Streben Sie die Schaffung einer gesetzlichen Grundlage für die Verwendung der AHVN13 als Personenidentifikator an?
    a. Falls ja, mit welchem Ziel, und wie hoch schätzen Sie den damit anfallenden Aufwand ein?
    b. Falls nein, warum nicht?

Abschlussfrage: Befürworten Sie die AHVN13 als einheitlichen, organisationsübergreifend genutzten Personenidentifikator?

Anhang 3: Interview Guide NL

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[17] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.
Objectives of this interview:

- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In the Netherlands the Citizen Service Number (BSN) has been introduced in 2007. It replaces the social security number and tax number (SoFi number). The SoFi number has been cancelled with effect from 6 January 2014. From this date on, all inhabitants must be registered at a municipality. The BSN is recorded in the Municipal Records Database (GBA) and is written on each person's passport, ID-card and driving license. Citizen Service numbers are also used to exchange patient information reliably and securely in the Electronic Patient Records Database (EPD). Since 1 June 2009, all care providers, needs assessment agencies and health insurers have had to refer to citizen service numbers when exchanging information about patients or clients. It is also used in the education sector.

In this respect, Switzerland would like to learn from the experiences of the Netherlands on their introduction of the BSN.

Interview Questions

1. Is the situation in the Netherlands as described above accurate?
2. Which processes and infrastructures have been cut after the introduction of the BSN (economic value)?
3. What values and benefits have been generated due to the introduction of the BSN (societal, cultural value)?
4. What have been main privacy concerns before the introduction of the BSN (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
5. What provisions have been installed to secure privacy (legal technical, organizational)?
6. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose.

[17] Assembly of cantonal ICT representatives

To be defined with interviewee at the beginning or end of the interview.

Follow Up
To be discussed directly after the interview.

Anhang 4: Interview Guide DK

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[18] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.
Objectives of this interview:

- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In Denmark, every resident person has a civil registration number. The number is registered in the Civil Registration System (the CPR). The CPR contains basic personal data (full name, address, date of birth, marital status, nationality, etc.) about anyone with a civil registration number. Registration is made by local authorities. Any person is entitled to protection of name and address, local directories protection, opt-out of statistical, scientific surveys and marketing approaches. Information from CPR can only be disclosed according to law (permission granted by law and compliant with the Processing of Personal Data Act). Public authorities address their inquiries for CPR-Data to local authorities. Private individuals or entities that can prove their legal interest can be granted access to CPR-data by the Ministry of Economic Affairs and the Interior. As a resident, their CPR-number is relevant to apply for a NemID, a common secure login on the Internet to engage with businesses or public authority online.

In this respect, Switzerland would like to learn from the experiences of Denmark on the net value of having a CPR-number.

Interview Questions

7. Is the situation in Denmark as described above accurate?
8. Which processes and infrastructures in e-government are simplified through the use of a unique identifier (economic value)? What are the main benefits for the collaboration between state levels?
9. What other values and benefits are generated through the CPR-number (societal, cultural value)?
10. What are the main privacy concerns with the use of a unique identifier (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
11. What provisions have been installed to secure privacy (legal technical, organizational)?
12. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

[18] Assembly of cantonal ICT representatives

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose.
To be defined with interviewee at the beginning or end of the interview.

Follow Up
To be discussed directly after the interview.

Anhang 5: Interview Guide ES

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[19] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.

Objectives of this interview:
- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In Spain, every citizen over 14 years has National ID Card (DNI) which contains a 8+1 Digit Personal identification number. The number is also referred to as National Fiscal Number (NIF). Minors and foreigners do also obtain a NIF, referred to as NIE. The first version of a national identification number has been introduced in 1944. The NIF/DNI in the current form has been created in 1990 and is widely used for identification purpose in transactions with private and public entities. A sector specific identification number has been created for the health sector, but the DNI is often used instead of the health identification number.

In this respect, Switzerland would like to learn from the experiences of Spain on the use and benefits of the DNI/NIF.

Interview Questions

13. Is the situation in Spain as described above accurate?
14. Which processes and infrastructures in e-government are simplified through the use of a unique identifier (economic value)? What are the main benefits for the collaboration between the different state levels/different provinces?
15. What other values and benefits are generated through the DNI (societal, cultural value)?
16. What are the main privacy concerns with the use of the DNI (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
17. What provisions have been installed to secure privacy (legal technical, organizational)?
18. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose.
To be defined with interviewee at the beginning or end of the interview.

[19] Assembly of cantonal ICT representatives

Follow Up
To be discussed directly after the interview.

Versionskontrolle

Version	Datum	Beschreibung	Autor
1.0	10.08.2015	Definitive Version Erstentwurf für Vernehmlassung in SIK-Arbeitsgruppe „AHV-Nummer als Identifikator“	Angelina Dungga Thomas Selzam Olivier Brian Katinka Weissenfeld Jérôme Brügger Andreas Spichiger
2.0	30.09.2015	Definitive Version	Angelina Dungga