Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

19.057

Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung

(Systematische Verwendung der AHV-Nummer durch Behörden)

vom 30. Oktober 2019

Sehr geehrte Frau Nationalratspräsidentin
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf einer Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung.

Gleichzeitig beantragen wir Ihnen, den folgenden parlamentarischen Vorstoss abzuschreiben:

2017	P	17.3968	Sicherheitskonzept für Personenidentifikatoren (N 19.09.18, Kommission für Rechtsfragen)

Wir versichern Sie, sehr geehrte Frau Nationalratspräsidentin, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

30. Oktober 2019

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ueli Maurer
Der Bundeskanzler: Walter Thurnherr

Übersicht

Die Verwaltungsabläufe sollen durch eine kontrollierte Verwendung der AHV-Nummer (AHVN) effizienter werden. Künftig sollen Behörden von Bund, Kantonen und Gemeinden die AHVN generell für die Erfüllung ihrer gesetzlichen Aufgaben systematisch verwenden dürfen. Dadurch können Verwechslungen bei der Bearbeitung von Personendossiers vermieden werden. Die Vorlage trägt somit zugleich zur erfolgreichen Umsetzung der Strategie «E-Government Schweiz» bei und erhöht auch die Kosteneffizienz der Verwaltungen.

Ausgangslage

Seit ihrer Einführung im Jahr 1948 arbeitet die AHV mit einer Versichertennummer. Dieses Personenkennzeichen hat bis heute den Zweck, die Verarbeitung von Informationen über Beiträge und die Berechnung damit verbundener Sozialversicherungsleistungen zu erleichtern. Im Jahr 2008 wurden eine nichtsprechende, 13-stellige AHVN neu eingeführt und zugleich die Zulässigkeit der systematischen Verwendung derselben neu geregelt. Die systematische Verwendung der AHVN ausserhalb der AHV ist seither nur unter bestimmten Voraussetzungen erlaubt. Zum einen sind die Stellen und Institutionen dazu befugt, die mit dem Vollzug von kantonalem Recht mit besonderem Bezug zu den Sozialversicherungen betraut sind. Zum anderen darf die AHVN systematisch verwendet werden, wenn eine spezialgesetzliche Grundlage des Bundes oder der Kantone besteht, die dazu ermächtigt. Die Bestimmung im jeweiligen Spezialgesetz hat Verwendungszweck und Nutzungsberechtigte zu nennen. Dies soll jeweils die demokratische Kontrolle ermöglichen.

Die systematische Verwendung der AHVN als Personenidentifikator erlaubt bei der Datenbearbeitung eine automatische, rasche und genaue Aktualisierung der Personenattribute bei Personenstandsänderungen. Dies garantiert die Datenqualität in den Benutzerregistern. Da die Nummer eindeutig ist, können ferner administrative Verwechslungen von Personendossiers und dadurch verursachte Verletzungen des Datenschutzes vermieden werden. Ausserdem steigert ihre Verwendung die Kosteneffizienz der Verwaltung, indem sie eine Vereinfachung der internen Prozesse und der Querprozesse zwischen Behörden ermöglicht. Im Zuge der zunehmenden Digitalisierung der Verwaltungstätigkeit seit der Einführung der Regelung im Jahr 2008 ist eine starke Ausweitung der systematischen Nutzung erfolgt.

Die geltende Regelung im Bundesgesetz über die AHV lässt eine systematische Verwendung der AHVN für Behörden zwar zu, wenngleich unter Voraussetzungen, die zu erfüllen als umständlich wahrgenommen wird. Zudem ist die Gesetzgebungspraxis hinsichtlich der Berechtigung zur systematischen Verwendung der AHVN widersprüchlich. Die Kantone können ihre Behörden ausserdem nur hinsichtlich des Vollzugs von kantonalem Recht zur Verwendung der AHVN ermächtigen. Aus diesen Gründen wird zunehmend gefordert, dass Behörden von Bund, Kantonen und Gemeinden die AHVN als eindeutigen Personenidentifikator nutzen dürfen.

Inhalt der Vorlage

Die Vorlage bezweckt, die Voraussetzungen dafür zu schaffen, dass die Behörden von Bund, Kantonen und Gemeinden nicht mehr für jede neue systematische Verwendung der AHVN eine spezifische gesetzliche Grundlage benötigen, sondern generell dazu ermächtigt sind. Indem für alle Behörden dieselben Verwendungsvoraussetzungen gelten, wird die Transparenz erhöht. Ferner sollen auch Organisationen und Personen, die keine Behördeneigenschaft besitzen und die ein Gesetz mit der Wahrnehmung einer Verwaltungsaufgabe betraut, zur systematischen Verwendung berechtigt sein, sofern eine Bestimmung im betreffenden Spezialgesetz dies vorsieht. Die systematische Verwendung rein privater Art der AHVN soll hingegen nach wie vor ausgeschlossen sein. Auch künftig soll es möglich sein, in spezialgesetzlichen Bestimmungen für bestimmte Verwendungszwecke sektorielle Personenidentifikatoren statt die AHVN vorzuschreiben. Insofern behält der Gesetzgeber die Gestaltungsfreiheit.

Die Vorlage beschränkt sich mithin darauf, zum einen das bisherige Erfordernis einer spezifischen gesetzlichen Grundlage für jede zusätzliche systematische Verwendung der AHVN durch eine generelle gesetzliche Berechtigung für die Behörden von Bund, Kantonen und Gemeinden und für bestimmte Institutionen zu ersetzen. Zum andern soll die Durchsetzung des Datenschutzes und der Informationssicherheit den erforderlichen Stellenwert erhalten. Die zur systematischen Verwendung der AHVN Berechtigten müssen verschiedene technische und organisatorische Massnahmen treffen. In erster Linie sind die Zugänge zu den verschiedenen Datenbanken optimal zu sichern, um das Risiko von unrechtmässigen Nutzungen zu minimieren. Die Sicherheitsvorgaben bezüglich Zugang zu Datenbanken, welche die AHVN enthalten, betreffen Authentifizierung, Datenübertragung, Verschlüsselung, Virenschutz und Firewalls sowie Aufzeichnung und Auswertung von wichtigen Abläufen innerhalb der Informatiksysteme. Indem die verwendenden Behörden zur Einhaltung dieser Begleitmassnahmen verpflichtet sind, dient die Vorlage auch der generellen Steigerung der Informationssicherheit in der öffentlichen Verwaltung.

Inhaltsverzeichnis

Übersicht **7360**

1 Ausgangslage **7364**

1.1 Handlungsbedarf und Ziele 7364
1.1.1 Bisherige Entwicklung 7364
1.1.2 Aktuelle Regelung 7365
1.1.3 Risikoanalyse in Erfüllung des Postulats 17.3968 Kommission für Rechtsfragen NR «Sicherheitskonzept für Personenidentifikatoren» 7366
1.1.4 Exkurs: Nutzung der amerikanischen Sozialversicherungsnummer 7374
1.2 Gewählte Lösung und geprüfte Alternativen 7375
1.2.1 Gewählte Lösung: Systematische Verwendung der AHVN durch alle Behörden 7375
1.2.2 Geprüfte Alternativen 7377
1.3 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrats 7378
1.3.1 Verhältnis zur Legislaturplanung 7378
1.3.2 Verhältnis zu Strategien des Bundesrates 7379
1.4 Erledigung parlamentarischer Vorstösse 7380

2 Vorverfahren, insbesondere Vernehmlassungsverfahren **7380**

2.1 Stellungnahme der Eidgenössischen AHV/IV-Kommission 7380
2.2 Vernehmlassungsverfahren 7380

3 Rechtsvergleich **7381**

4 Grundzüge der Vorlage **7381**

4.1 Die beantragte Neuregelung 7381
4.2 Begleitmassnahmen 7382
4.3 Keine Pflicht zur Neukonzeption der Datenbankarchitektur 7382
4.4 Unveränderte Bestimmungen über Schweigepflicht der Behörden und Datenbekanntgabe 7383
4.5 Abstimmung von Aufgaben und Finanzen 7384
4.6 Umsetzungsfragen 7384

5 Erläuterungen zu einzelnen Artikeln **7385**

5.1 Bundesgesetz über die Alters- und Hinterlassenenversicherung 7385
5.2 Koordinationsbedarf mit anderen Revisionsvorlagen 7392

6 Auswirkungen **7392**

6.1 Finanzielle und personelle Auswirkungen auf den Bund 7392
6.2 Finanzielle und personelle Auswirkungen auf Kantone und Gemeinden 7393

6.3 Auswirkungen auf die Volkswirtschaft 7394
6.4 Auswirkungen auf die Gesellschaft 7394
6.5 Auswirkungen auf die Umwelt 7394

7 Rechtliche Aspekte 7394

7.1 Verfassungsmässigkeit 7394
7.1.1 Kompetenzen 7394
7.1.2 Persönlichkeitsschutz 7394
7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz 7395
7.3 Erlassform 7395
7.4 Unterstellung unter die Ausgabenbremse 7395
7.5 Delegation von Rechtsetzungsbefugnissen 7395

Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG) *(Entwurf)* **7379**

Botschaft

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

1.1.1 Bisherige Entwicklung

Die Alters- und Hinterlassenenversicherung (AHV) arbeitet seit ihrer Einführung im Jahr 1948 mit einer AHV-Nummer (AHVN). Bis heute hat dieser Personenidentifikator den Zweck, die Verarbeitung von Informationen über Beiträge und die Berechnung damit verbundener Sozialversicherungsleistungen zu erleichtern. Die AHVN war ursprünglich «sprechend»: Aus der Nummer konnten jeweils die Anfangsbuchstabengruppe des Namens, das Geburtsdatum und das Geschlecht abgeleitet werden. Aus datenschutzrechtlicher Sicht erwies sich dies als unbefriedigend. Im Laufe der Zeit war es ausserdem zu Engpässen bei der Vergabe der AHVN gekommen, was zu erheblichen informationstechnischen Problemen führte. Die Verwaltung der AHVN war zudem fehleranfällig, weil die Nummer bei Personenstandsänderungen der versicherten Person jeweils Änderungen erfuhr. Im Rahmen der Vernehmlassung zum Registerharmonisierungsgesetz[1] im Jahre 2003 wurde deshalb die Einführung eines verwaltungs- und registerübergreifenden eidgenössischen Personenidentifikators (EPID) vorgeschlagen. Aufgrund der Bedenken seitens der Datenschutzkreise schlug der Bundesrat in einer weiteren Vernehmlassung im Sommer 2004 sechs sektorielle Personenidentifikatoren (SPIN) mit einem zentralen Identifikations- und Kommunikationsserver vor. Pro Verwaltungssektor, darunter die Sozialversicherungen, sollte ein einheitlicher Personenidentifikator verwendet werden. Die Vernehmlassungsergebnisse zeigten allerdings deutlich, dass sektorielle Personenidentifikatoren bei den Kantonen keine Mehrheit finden würden. Stattdessen wurde eine Lösung mit einer nichtsprechenden, 13-stelligen AHVN eingeführt, die zugleich auch Regelungen über die Voraussetzungen einer systematischen Verwendung dieser Nummer zu administrativen Zwecken ausserhalb der AHV enthielt.[2]

Im Zuge der fortschreitenden Digitalisierung der Verwaltungstätigkeit ist seit der Einführung der neuen AHVN im Jahr 2008 eine starke Ausweitung der systematischen Verwendung derselben ausserhalb der AHV zu beobachten, dies sowohl auf der Ebene des Bundes als auch auf derjenigen der Kantone. Gegenwärtig sind der Zentralen Ausgleichsstelle (ZAS) rund 12 700 Nutzer gemeldet. Zudem verwenden rund 60 000 Leistungserbringer die AHVN für die Rechnungsstellung in der obligatorischen Krankenpflegeversicherung.

Zahlreiche Akteure vertreten die Auffassung, die Anforderungen an die Befugnis zur systematischen Verwendung der AHVN seien zu lockern. So hat die Konferenz der kantonalen Finanzdirektorinnen und Finanzdirektoren im Januar 2014 angeregt, die AHVN sei als allgemeiner Personenidentifikator zur Verfügung zu stellen, damit E-Government-Projekte vorangetrieben werden könnten. Die Verwendung eines ein-

1 SR **431.02**
2 AS **2007** 5259

deutigen Personenidentifikators ermögliche eine effiziente Verwaltungsführung und erhöhe zugleich die Qualität der Datenbanken, indem die bisherigen Verwechslungsgefahren vollständig wegfielen. Auch bei der Ausarbeitung des Bundesgesetzes vom 18. Dezember 2015[3] über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) wurde auf Anregung der Kantone beschlossen, zur Vermeidung zusätzlicher administrativer Belastungen keine neue Steueridentifikationsnummer zu schaffen, sondern vielmehr die AHVN als Steueridentifikationsnummer heranzuziehen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) und ein Teil der kantonalen Datenschutzbeauftragten stehen dieser Entwicklung kritisch gegenüber, weil sie Gefahren für den Datenschutz befürchten.

Vor diesem Hintergrund hat der Bundesrat das Eidgenössische Departement des Innern im Februar 2017 damit beauftragt, ihm eine Änderung der AHVG-Bestimmungen zu unterbreiten, um den Bundes-, Kantons- und Gemeindebehörden die systematische Verwendung der AHVN bei der Erfüllung ihrer gesetzlichen Aufgaben zu erleichtern.

Vorliegend geht es darum, die gesetzlichen Grundlagen zu schaffen, die eine zukunftstaugliche Verwendung der AHVN ermöglichen und zugleich den Datenschutz gewährleisten.

1.1.2 Aktuelle Regelung

Die systematische Verwendung der AHVN ausserhalb der AHV ist aktuell wie folgt geregelt: Besteht für den Vollzug von Bundesrecht ein Bedarf nach systematischer Verwendung der AHVN, gibt es die Möglichkeit, eine hinreichende gesetzliche Grundlage ins jeweilige Bundesgesetz aufzunehmen. Die betreffende Gesetzesbestimmung hat die ermächtigten Nutzerinnen und Nutzer und den Verwendungszweck zu bestimmen (Art. 50*d* Abs. 1 und 50*e* Abs. 1 des Bundesgesetzes vom 20. Dezember 1946[4] über die Alters- und Hinterlassenenversicherung [AHVG]). Indem der Gesetzgeber im jeweiligen Spezialgesetz die Berechtigung erteilt, ist die betreffende systematische Verwendung demokratisch abgestützt. Dieselben Voraussetzungen gelten grundsätzlich auch für eine Verwendung zum Vollzug von kantonalem Recht (Art. 50*d* Abs. 1 und 50*e* Abs. 3 AHVG), mit Ausnahme der vier Bereiche Prämienverbilligung, Sozialhilfe, Steuern und Bildungsinstitutionen. Hier ist die Berechtigung zur Verwendung durch kantonale Stellen bereits im AHV-Recht enthalten (Art. 50*e* Abs. 2 AHVG), es bedarf also keiner zusätzlichen Grundlage in einem kantonalrechtlichen Spezialgesetz. Rein private systematische Nutzungen sind grundsätzlich nicht zulässig. Allerdings wird die AHVN im Rahmen des automatischen Informationsaustauschs in Steuersachen systematisch als Steueridentifikationsnummer im grenzüberschreitenden Datenaustausch verwendet. Sie wird seit Herbst 2018 an Finanzinstitute in über 50 Staaten und Territorien übermittelt.

Die Stellen, welche die AHVN systematisch zu verwenden beabsichtigen, die aber nicht den Sozialversicherungen des Bundes angehören, haben sich vorgängig der

3 SR **653.1**
4 SR **831.10**

ZAS zu melden. Sind sie zur systematischen Verwendung ermächtigt, erhalten sie anschliessend Zugriff auf die von der ZAS betriebene UPI-Datenbank. Die UPI-Datenbank (UPI steht für «Unique Person Identification») ist eine von der ZAS geführte Personendatenbank, die ausschliesslich zur Personenidentifikation dient. Sie enthält keinerlei Sachdaten. Jede Person, die eine AHVN erhalten hat, ist in der UPI-Datenbank auf eindeutige Art und Weise aufgeführt. Neben der AHVN enthält diese Datenbank die offiziellen Identitätsmerkmale einer natürlichen Person (offizieller Name, Ledigenname, offizielle Vornamen, Geburtsdatum, Geschlecht, Nationalität, Geburtsland und -ort, Name und Vorname von Vater und Mutter). Die ZAS kann die Aktualität, Vollständigkeit und Eindeutigkeit der in der UPI-Datenbank geführten Daten sicherstellen, indem sie diese von zahlreichen Quellen bezieht. Die wichtigsten Datenbezugsquellen sind die Durchführungsorgane der 1. Säule der schweizerischen Sozialversicherung sowie die zentralen Personenregister des Bundes Infostar (Informatisiertes Standesregister zur Beurkundung des Personenstandes), ZEMIS (Zentrales Migrationsinformationssystem für den Ausländer- und Asylbereich), E-VERA (Informationssystem Vernetzte Verwaltung der Auslandschweizerinnen und Auslandschweizer) und ORDIPRO (Informationssystem Verwaltung der ausländischen Diplomaten und internationalen Funktionäre). Hinzu kommen die kantonalen und kommunalen Einwohnerregister, Krankenkassen und andere Verwender der AHVN. Die Zugriffsberechtigten müssen im Interesse des Datenschutzes und der Datenqualität technische und organisatorische Massnahmen treffen, die auf Verordnungsebene geregelt sind.[5]

Das aktuelle System überlässt den Entscheid über die Befugnis zur systematischen Verwendung der AHVN ausserhalb der AHV dem zuständigen Gesetzgeber. Dieser erteilt die diesbezügliche gesetzliche Ermächtigung anhand einer allgemeinen Einschätzung der Informationssicherheit im betreffenden Bereich.

1.1.3 Risikoanalyse in Erfüllung des Postulats 17.3968 Kommission für Rechtsfragen NR «Sicherheitskonzept für Personenidentifikatoren»

Die nachfolgenden Ausführungen erfolgen in Erfüllung des Postulats 17.3968 der Rechtskommission des Nationalrats vom 20. Oktober 2017, das der Nationalrat im September 2018 angenommen hat. Es steht im Zusammenhang mit der parlamentarischen Beratung zur Modernisierung des Grundbuches[6] und einer im September 2017 durchgeführten Risikoanalyse[7]. Das Postulat beauftragt den Bundesrat, innerhalb der laufenden Legislatur in einem Konzept aufzuzeigen, wie den Risiken begegnet werden könne, die mit der Verwendung der dreizehnstelligen AHVN als einziger

5 Verordnung des EDI über die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der AHVN ausserhalb der AHV; SR **831.101.4.**

6 www.parlament.ch > 14.034 (ZGB. Beurkundung des Personenstands und Grundbuch)

7 «Risikoanalyse zur unterschiedlichen Verwendung der schweizerischen AHV-Nummer», ETH Zürich, Institut für Informationssicherheit, Prof. Dr. David Basin, Zürich, 2017; vgl. www.derbeauftragte.ch, Datenschutz – Statistik, Register, Forschung – AHV-Nummer.

Personenidentifikationsnummer verbunden sind. Zudem sei aufzuzeigen, wie der Datenschutz bei der Verwendung von Personenidentifikationsnummern durch Kantone, Gemeinden und Dritte verbessert werden könne und die Beurteilung des EDÖB zu berücksichtigen.

Einleitende Vorbemerkung

Regelmässig zeigt sich, dass Unklarheiten bezüglich der Beschaffenheit und der Funktion von Personenidentifikatoren bestehen. Ausserdem kursieren zahlreiche, teils unzutreffende Annahmen von den Gefahren, die von der systematischen Verwendung von Personenidentifikatoren im Allgemeinen und der AHVN im Besonderen ausgehen. Vor diesem Hintergrund verlangt das Postulat eine Klärung der Situation. Moderne Identifikatoren wie die AHVN sind nichtsprechend. Sie ermöglichen weder den Zugang zu IT-Systemen noch dienen sie zur Authentifikation im Internet (sog. E-ID). Die einzige Gefahr für den Datenschutz, die die systematische Verwendung von eindeutigen Personenidentifikatoren im Grundsatz tatsächlich enthält, liegt in der Möglichkeit, anhand des Personenidentifikators Persönlichkeitsprofile zu bilden, die präziser ausfallen als jene, die anhand von anderen, öffentlich zugänglichen oder dem Ersteller bekannten Merkmalen gebildet werden können. Unter einem Persönlichkeitsprofil versteht man eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Nachfolgend wird darzulegen sein, inwieweit dieses Risiko besteht. Ausserdem sind die Ansätze zu erläutern, wie dieses Risiko auf ein vernünftiges und durchführbares Mass minimiert werden kann. Aufgabe des Gesetzgebers ist es hingegen, zu beurteilen, ob – und gegebenenfalls, unter welchen Rahmenbedingungen – der Nutzen der systematischen Verwendung der AHVN das Restrisiko überwiegt.

Definition und Funktion von Personenidentifikatoren

Ein Personenidentifikator dient dazu, die einzelnen Informationen innerhalb einer Sammlung von Personendaten richtig zuzuordnen. Anders als die übrigen Attribute wie Name oder Vorname, die mehrfach vorkommen können, ermöglicht ein einmaliger Identifikator eine eindeutige Zuordnung von Datensätzen und Personen. Indem Verwechslungen von Dossiers ausgeschlossen sind, steigt die Datenqualität in den Registern.

Wie andere Personenidentifikatoren des Bundes dient auch die AHVN ausschliesslich dazu, innerhalb einer Datensammlung einen Satz von Personendaten der richtigen Einzelperson zuordnen zu können. Sie wird nur zu administrativen Zwecken verwendet. Eine AHVN wird jeder natürlichen Person kurz nach der Geburt auf Schweizer Territorium bzw. nach Begründung von Wohnsitz oder gewöhnlichem Aufenthalt in der Schweiz zugeteilt. Sie ist eine einmalige, lebenslang unveränderliche Personenidentifikationsnummer. Mehrfachvergaben sind zwar nicht ausgeschlossen, die heutigen Kontrollmechanismen sind jedoch so streng, dass solche Fehler selten vorkommen und schnell entdeckt und bereinigt werden. Die ZAS meldet annullierte oder deaktivierte AHV-Nummern laufend an ihre Nutzer, damit sie ihre Datenbanken entsprechend aktualisieren.

Betrachtet man die im Bundesrecht geregelten Register unter dem Aspekt der verwendeten Personenidentifikatoren, zeigt sich ein uneinheitliches Bild. Auch aus-

serhalb der Sozialversicherungen gibt es Personenregister, die als Personenidentifikator nur die AHVN führen, so etwa das zentrale Dosisregister von beruflich strahlenexponierten Personen.[8] Andere zentrale Register des Bundes, so z. B. ZEMIS, E-VERA oder ORDIPRO, verwenden zusätzlich zu eigenen, registerspezifischen Personenidentifikatoren auch die AHVN. Dasselbe gilt für das eidgenössische Medizinalberuferegister[9] und das Gesundheitsberuferegister.[10] Das Bundesrecht sieht auch vor, dass die AHVN den kantonalen Handelsregisterbehörden zur Identifizierung von natürlichen Personen dient. Zusätzlich wird den Personen, die in der zentralen Datenbank Personen erfasst sind, eine registerspezifische Nummer zugeteilt.[11] Die eindeutige Patienten-Identifikationsnummer für das elektronische Patientendossier (EPD) ist eine registerspezifische Nummer, die von der ZAS ausgegeben und verwaltet wird; dort ist sie an die AHVN angebunden.[12]

Die Unternehmensidentifikationsnummer (UID) ist nicht ein Personenidentifikator im engeren Sinne, zumal auch den Personengemeinschaften ohne Rechtspersönlichkeit zugeteilt wird.[13] Gleiches gilt für das Betriebs- und Unternehmensregister (BUR), das die Daten über die in der Schweiz domizilierten Unternehmen und Betriebe des privaten und öffentlichen Rechts enthält.[14]

Keine Rückschlüsse auf die Person durch die AHVN

Nur «sprechende» Personenidentifikatoren lassen Rückschlüsse auf die Person zu. Ein Personenidentifikator gilt dann als sprechend, wenn er kodierte Informationen über Zivilstand, Alter, Geschlecht oder andere persönliche Eigenschaften der Trägerin oder des Trägers enthält. Dies kann zu einer unerwünschten Preisgabe von Personendaten führen. Zudem treten Schwierigkeiten auf, sobald Personendaten (z. B. der Familienname) ändern. Ist ein Personenidentifikator hingegen zufällig oder als fortlaufende Systemnummer generiert, enthält er keine kodierte Information über deren Trägerin oder Träger und gilt als nichtsprechend.[15] Die auf Bundesebene gebräuchlichen Identifikatoren sind ausschliesslich als nichtsprechende Nummern ausgestaltet.[16] Die AHVN enthält keine Informationen über die Inhaberin oder den Inhaber und erlaubt demzufolge keine Rückschlüsse auf deren oder dessen persönliche Eigenschaften. Dies im Unterschied zur 11-stelligen Nummer, die von der heute

8 Art. 72–76 der Strahlenschutzverordnung vom 26. April 2017; SR **814.501.**
9 Art. 51 Abs. 4bis des Medizinalberufegesetzes vom 23. Juni 2006 (MedBG); SR **811.11.**
10 Art. 24 Abs. 3 des Gesundheitsberufegesetzes vom 30. September 2016 (GesBG); BBl **2016** 7599; noch nicht in Kraft.
11 nArt. 928*c* Abs. 1 und 3 OR; BBl **2017** 2435; noch nicht in Kraft.
12 Art. 4 und 5 Abs. 1 des Bundesgesetzes vom 19. Juni 2015 über das elektronische Patientendossier (EPDG); SR **816.1.**
13 UID-Einheiten gemäss Art. 3 Abs. 1 Bst. c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG); SR **431.03.**
14 Art. 3 Abs. 1 der Verordnung vom 30. Juni 1993 über das Betriebs- und Unternehmensregister (BURV); SR **431.903.**
15 Art. 25 Abs. 1 zweiter Satz der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (SR **235.11**) lautet: «Eine nichtsprechende Nummer ist jede eindeutige oder umkehrbar eindeutige Summe von Zeichen, die jeder Person, die in einer Datensammlung registriert ist, zugeteilt wird, und aus der keine Rückschlüsse auf die Person gezogen werden können.».
16 Als Identifikator i. S. des Registerharmonisierungsgesetzes (RHG; SR **431.02**) gilt eine Nummer, wenn sie nicht sprechend und unveränderlich ist (Art. 3 Bst. e RHG).

verwendeten, 13-stelligen Nummer abgelöst wurde (vgl. Ziff. 1.1.1). Um die schweizerische Herkunft der Nummer sichtbar zu machen, beginnen sämtliche AHVN mit dem Präfix «756» für die Landesidentifikation gemäss ISO 3166. Die Stellen 4 bis 12 enthalten eine Zufallszahl im Bereich zwischen 0 und 999 999 999, die aus den noch nicht verbrauchten Zahlen gezogen wird. Stelle 13 enthält die Prüfziffer.

Die AHVN ist kein Authentifikator

Der Prozess der Authentisierung oder Authentifikation garantiert, dass eine Person tatsächlich diejenige ist, welche sie zu sein erklärt. Bei der Authentifikation anhand eines Passworts fordert das System die Nutzerin oder den Nutzer auf, die Richtigkeit ihrer oder seiner Behauptung zu beweisen, indem sie oder er eine Angabe macht, von der nur sie oder er Kenntnis hat (wissensbasierte Authentifizierung). Die Nennung seiner AHVN steht dazu nicht zur Verfügung.

Bei den allgemeinen Büroanwendungen der öffentlichen Verwaltungen erfolgt die Überprüfung von Zugriffsrechten in der Regel über eine Zwei-Faktor-Authentisierung (z. B. «Smartcard» des Bundes in Kombination mit persönlichem Passwort). Für die Nutzung von Fachanwendungen – namentlich von solchen, die den Zugang zu Personendaten gewähren – werden zusätzliche, anwendungsspezifische Anmeldungsdaten benötigt (Benutzercode und Passwort). Die AHVN ist kein Benutzercode oder Passwort, mit dem man sich Zugriff zu Informatiksystemen verschaffen kann. Hat man Kenntnis von einem Personenidentifikator wie der AHVN, hat dies daher nicht zur Folge, dass man in ein Informatiksystem eindringen kann, auf das man andernfalls keinen rechtmässigen Zugriff hätte. Die systematische Verwendung von Personenidentifikatoren in einer Datensammlung führt also nicht zu einer erhöhten Verwundbarkeit derselben. Sie ist auch kein (digitaler) Identitätsnachweis, z. B. im Rahmen der Internetnutzung. Staatliche Leistungen zu erhalten, indem man einzig eine AHVN angibt, ist somit ausgeschlossen. Allein aus der Kenntnis der eigenen oder einer fremden AHVN lässt sich weder ein finanzieller noch ein immaterieller Nutzen ziehen.

Die AHVN gibt keinen erweiterten Zugriff auf andere Datenbanken

Eine Behörde, die zur Verwendung der AHVN befugt ist, darf den üblichen Attributen wie Name oder Geburtsdatum der registrierten Personen deren jeweilige AHVN hinzufügen. In der Datenbank sind die Sachdaten einer Person dann in erster Linie dieser Nummer zugeordnet. Um sicherstellen zu können, dass sie die richtige Nummer verwendet oder dass die übrigen Attribute korrekt sind, hat die Behörde Zugriff auf die UPI-Datenbank. Sie erhält dadurch jedoch keinen Zugriff auf die übrigen Register, namentlich nicht auf das zentrale Versichertenregister und das Leistungsregister der ZAS, oder auf Register mit Sachdaten, die von anderen Behörden geführt werden. Die Berechtigung, die AHVN zu verwenden, verschafft einer Behörde also keine Verknüpfungsmöglichkeit oder -berechtigung (zur Verknüpfung vgl. sogleich unten).

Verknüpfungen anhand von Personenidentifikatoren; Persönlichkeitsprofile

Durch Verknüpfung der in verschiedenen Systemen enthaltenen Daten können mehrere Merkmale derselben Person zu einem sogenannten Persönlichkeitsprofil zusammengefasst werden. Ein solches enthält einerseits die grundlegenden Identitätsmerkmale einer Person wie Namen, Vornamen und Geburtsdatum, und zudem – je nach Inhalt der angegriffenen Datenbank – andere personenbezogene Informationen wie beispielsweise Gesundheits- oder Steuerdaten und dergleichen mehr. Unzulässige und daher unerwünschte Verknüpfungen sind technisch dann machbar, wenn es Angreifern gelingt, in mehrere Datenbanken einzudringen. Wird in mehreren Datenbanken derselbe, eindeutige Personenidentifikator verwendet, verbessert eine Verknüpfung anhand dieses Identifikators zwar – in geringem Ausmass – die Genauigkeit der Verknüpfungsresultate. Verknüpfungen sind aber auch ohne Personenidentifikatoren technisch machbar, z. B. anhand von Quasi-Identifikatoren wie Name und Vorname. Sie werden durch die Verwendung von Personenidentifikatoren auch nicht erleichtert.

Persönlichkeitsprofile können kommerziell genutzt werden. Je nachdem, wie detailliert und individualisiert die Profile sind, kann es lukrativ sein, damit Handel zu treiben. Käufer von Persönlichkeitsprofilen verfolgen in der Regel das Ziel, ihren Kundenstamm oder ihre Kenntnisse über ihre Kundinnen und Kunden zu erweitern. Auch Bonitätsdatenbanken, welche die Kreditwürdigkeit von Personen beurteilen, sind an Persönlichkeitsprofilen interessiert. Vorsicht ist überdies geboten, wenn staatliche Akteure Persönlichkeitsprofile aus digital gespeicherten Daten erstellen. Geschieht dies im Rahmen von gesetzlich geordneten und demokratisch legitimierten Prozessen – etwa zu statistischen Zwecken oder um klar formulierte wissenschaftliche Fragen beantworten zu können – ist dies unbedenklich. Um allfällige Probleme zu verhindern, dürfen Behörden Persönlichkeitsprofile (z. B. zu statistischen Zwecken) nur mit einer ausdrücklichen gesetzlichen Grundlage erstellen.

Ein Persönlichkeitsprofil kann ferner missbraucht werden, um einen sogenannten Daten- oder Identitätsdiebstahl zu begehen. Wird umgangssprachlich von Datendiebstahl gesprochen, ist gemeinhin das unbefugte Erlangen von Informationen gemeint. Bezieht sich die Information auf eine bestimmte Einzelperson und werden die Informationen in der Folge missbräuchlich verwendet, so spricht man über Identitätsdiebstahl oder Identitätsmissbrauch. Dabei wird eine fremde Identität vorgespiegelt, um an Leistungen zu gelangen, auf die kein Anrecht besteht; zugleich wird die Feststellung der tatsächlichen Identität erschwert oder verunmöglicht. Persönliche Daten, die in ihrer Gesamtheit eine «Identität» darstellen, sind beispielsweise der Name und der Vorname, das Geburtsdatum, die Nummern von Ausweisen, Bankkonten oder Kreditkarten sowie Computer-Passwörter, Zugangscodes oder sogenannte Nicknames. Die Vorspiegelung einer fremden Identität gelingt umso eher, je mehr Informationen dem Täter zur Verfügung stehen. Identitätsmissbrauch wird häufig mit dem Ziel betrieben, jemanden in seinem Ruf zu schädigen oder sich einen unrechtmässigen Vermögensvorteil zu verschaffen. Ob dem Täter dies gelingt, hängt unter anderem auch davon ab, ob sein Gegenüber auf einer Authentifizierung durch einen amtlichen Ausweis oder eine E-ID besteht. Die Kenntnis von einem Personenidentifikator allein ermöglicht noch keinen Datendiebstahl.

Eintrittswahrscheinlichkeit und potenzielles Schadenausmass

Alle behördlichen Personenregister enthalten notwendigerweise Identitätsattribute (wie Namen, Vornamen und Geburtsdatum) der registrierten Personen. Dabei handelt es sich um sogenannte Quasi-Identifikatoren. Gelingt es einer unbefugten Person (oder einer Software), in mehrere Datenbanken einzudringen, so kann sie die darin enthaltenen Personendaten bereits anhand der Quasi-Identifikatoren verknüpfen, also auch dann, wenn in diesen Datenbanken kein eigentlicher Personenidentifikator wie die AHVN verwendet wird. Je nachdem, welche Identitätsattribute in den Datenbanken verwendet werden, fällt der Zuverlässigkeitsfaktor jedoch unterschiedlich aus: Sind nur Name und Vorname gespeichert, liegt die Genauigkeit der Verknüpfungen bei 75,89 Prozent. Verwendet ein Personenregister hingegen Name, Vorname und Geburtsdatum, steigt deren Genauigkeit auf 99,98 Prozent.[17] Werden die Daten nicht anhand der genannten Identitätsattribute, sondern anhand eines eindeutigen Identifikators wie der AHVN verknüpft, resultiert eine Genauigkeit von 100 Prozent. Gegenüber einer Verknüpfung anhand von Name, Vorname und Geburtsdatum beträgt der Präzisionszuwachs somit 0,02 Prozent. Vorliegend geht es (nur) um das Risiko, das (ausschliesslich) dadurch entsteht, dass in einem Personenregister zusätzlich zu den bereits verwendeten Quasi-Identifikatoren neu auch die AHVN – und damit ein eindeutiger Personenidentifikator – gespeichert wird.

Es stellt sich also die Frage, ob allein der Genauigkeitsgewinn von 0,02 Prozent dazu führt, dass unbefugte Personen in Datenbanken eindringen oder einzudringen versuchen, um unerlaubte Persönlichkeitsprofile zu bilden, die sie andernfalls nicht erstellt hätten, oder um bereits von ihnen erstellte Persönlichkeitsprofile zu verbessern oder zu ergänzen. Mit anderen Worten: Ist anzunehmen, dass Unbefugte im erwähnten Präzisionszuwachs von 0,02 Prozent einen entscheidenden Anreiz sehen? Ob dieser Zuwachs an Genauigkeit unbefugte Personen tatsächlich dazu bewegt, widerrechtlich in Informationssysteme einzudringen oder dies zu versuchen, kann hier nicht abschliessend beurteilt werden. Schweizerische Personendatenbanken haben auch ohne Verwendung eines Personenidentifikators wie die AHVN schon eine hohe Präzision und könnten daher grundsätzlich interessant sein. Auf jeden Fall hängt es massgeblich vom jeweiligen Stand der Informationssicherheitsmassnahmen ab, ob es Unbefugten gelingt, einzudringen oder nicht. Entscheidend ist also in erster Linie, welcher Aufwand zu treiben ist, um ein System erfolgreich anzugreifen. Anders formuliert: Je besser ein System gesichert ist, desto weniger bildet der jeweilige Genauigkeitszuwachs einen Anreiz, dieses anzugreifen. Ist die Informationssicherheit gewährleistet, sind Daten- bzw. Identitätsdiebstähle und unerlaubte Profilbildungen ausgeschlossen. Ist sie jedoch mangelhaft, steigt das Risiko. Falls unter den registrierten Daten auch ein Personenidentifikator figuriert, ist dies für die Frage der Verwundbarkeit eines Informatiksystems hingegen bedeutungslos.

Zur Bewertung eines Risikos wird die Eintrittswahrscheinlichkeit eines Ereignisses der Schwere des Schadens gegenübergestellt, der aus dem Ereignis resultieren würde. Ob infolge einer gegenüber heute etwas breiteren systematischen Verwendung der AHVN anhand dieser Nummer unerlaubte Profile gebildet werden, ist nicht genau voraussehbar. Die Wahrscheinlichkeit ist aber sehr gering, da Unbefugte

17 Vgl. Basin, a.a.O., Ziff. 2.2.3, S. 11.

auch ohne diese AHVN Persönlichkeitsprofile mit einer hohen Präzision bilden oder Daten stehlen können, sofern es ihnen gelingt, in (mehrere) geeignete Datenbanken einzudringen. Auch die Schwere von möglichen Persönlichkeitsverletzungen durch unerlaubte Profilbildung kann nicht generell beurteilt werden. Diese hängt davon ab, welche Art von Personendaten konkret miteinander verknüpft werden. Werden allgemein zugängliche Daten verknüpft (etwa Wohnadressen mit Daten zum Geschlecht), ist dies weit weniger einschneidend als beispielsweise eine unerlaubte Verknüpfung von Daten aus dem Gesundheitsbereich mit solchen zu allfälligen Vorstrafen. Werden die Vorgaben bezüglich IT-Sicherheit konsequent eingehalten, so liegt die Eintrittswahrscheinlichkeit aber im einen wie im andern Fall ausgesprochen tief.

Massnahmen

Massnahmen gegen unrechtmässiges Eindringen von Angreifern

Die Schaffung von Informatiksicherheit ist keine Einzelmassnahme, sondern ein immerwährender Prozess, der die kontinuierliche Betrachtung und Anpassung verschiedener Faktoren erfordert. Um zu verhindern, dass Unbefugte («Hacker») in Informatiksysteme eindringen, diese ausspähen und die darin gespeicherten Informationen verknüpfen, müssen die Prozesse und Sicherheitsverfahren permanent auf dem neusten Stand gehalten werden. Insbesondere, wenn Personendaten in Informatiksystemen gespeichert sind, bedarf es ständiger minutiöser Kontrollen derselben. Das Hauptaugenmerk ist darauf zu richten, dass die Datenbanken vor nicht berechtigter Einsichtnahme und Manipulation gesichert sind. Die vom Bund betriebenen Datenbanken und Fachapplikationen weisen insgesamt ein vergleichsweise hohes Sicherheitsniveau auf. Dasselbe gilt für zahlreiche IT-Systeme von Kantonen und Gemeinden. Dennoch gibt es ausserhalb der Bundesverwaltung etliche Systeme, die den aktuellen Sicherheitsstandards nicht ganz genügen. Diese Situation muss mit Hilfe von Sicherheitsmassnahmen behoben werden. Ein hinreichendes Sicherheitsniveau kann nur durchgesetzt werden, wenn organisatorische, personelle, infrastrukturelle und technische Vorgaben eingehalten werden.

Konkret bedeutet dies zunächst, dass die Verantwortlichkeiten bezüglich der IT-Sicherheit geregelt sein müssen. Für die Abgrenzung der Aufgabengebiete, aber auch zur Vermeidung von Zuständigkeitslücken müssen die Verantwortlichkeiten für alle wesentlichen Aufgaben, insbesondere im Informationssicherheitsprozess, nachvollziehbar geregelt sein. Mitarbeitende, die mit Informatikmitteln zu tun haben, müssen im Umgang mit der IT-Infrastruktur hinsichtlich der IT-Sicherheit geschult sein. Sicherheitsrichtlinien und -anweisungen müssen in schriftlicher Form dokumentiert werden. Die Risiken im Bereich Informationssicherheit sind regelmässig zu prüfen, und es ist ein Informationssicherheits- und Datenschutzkonzept (ISDS) zu erstellen. Was die physische Sicherung angeht, ist einerseits der Zugang zu Informatikmitteln und Datenspeichern zu sichern. Vor der Reparatur, Entsorgung oder Vernichtung derselben ist anderseits sicherzustellen, dass sie weder AHVN noch andere Personendaten mehr enthalten und dass solche Daten auch nicht rekonstruiert werden können.

Des Weiteren müssen die technischen Zugriffsrisiken minimiert werden. Dazu gehören geeignete Authentisierungsverfahren sowie Informatiksicherheitsmassnah-

men (Antiviren-Software, Firewall-Systeme). Die Software muss dem Stand der Technik entsprechen und regelmässig anhand von Sicherheitsupdates und Fehlerbehebungs-Patches aktualisiert werden. Bei mobilen Netzen sind die Daten mit kryptografischen Verfahren zu verschlüsseln, die dem neusten Stand der Technik entsprechen. Werden Log-Daten der Rechner regelmässig und systematisch ausgewertet, können Abweichungen oder Störungen im laufenden Betrieb der IT-Systeme identifiziert werden, die auf fehlenden bzw. fehlerhaften Programmen basieren oder durch Sicherheitslücken zustande kommen. Sicherheitsvorfälle müssen schnell und effizient bearbeitet werden, um das Ausspähen, die Manipulation oder die Zerstörung von Daten zu vermeiden oder zu begrenzen. Als Sicherheitsvorfall wird dabei ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge grosse Schäden nach sich ziehen kann. Gibt es hierzu ein vorgegebenes und erprobtes Verfahren, so kann dies dazu beitragen, Reaktionszeiten zu verringern. Die Behandlung von Sicherheitsvorfällen ist daher im Vorfeld zu konzipieren und einzuüben.

Massnahmen gegen unzulässige staatliche Datenbearbeitung

Das Prinzip der Verhältnismässigkeit der Datenbearbeitung schreibt vor, dass jeder behördliche Dienst grundsätzlich nur auf die Daten zugreifen kann, für die er direkt zuständig ist. Ausserdem ist darauf zu achten, dass nur die Daten gesammelt werden, welche die Behörden tatsächlich benötigen. Die Datenaustauschprozesse dürfen überdies nicht beliebig ausgeweitet werden. Diesen Anliegen, die grundlegende Prinzipien des Datenschutzrechts darstellen, ist im Rahmen der Gesetzgebung zu den einzelnen Registern Rechnung zu tragen.

Die Vernetzung der behördlichen Informationssysteme untereinander nimmt allerdings laufend zu. Wo diesbezügliche gesetzliche Grundlagen bestehen, tauschen die dazu berechtigten Behörden regelmässig Informationen untereinander aus. Einerseits werden Informationssysteme von unterschiedlichen Behörden über Schnittstellen miteinander verbunden, anderseits erhalten Behörden Zugriffsrechte auf Datenbanken anderer Behörden, die sie im Abrufverfahren ausüben können. Als Abrufverfahren gilt ein automatisiertes Verfahren, bei dem sich eine Person die Information selbst beschaffen kann, ohne dass die Verwaltung davon überhaupt Kenntnis hat oder Kenntnis zu nehmen braucht. Zum Teil geht die Tendenz auch dahin, die Bearbeitung der Daten zu konzentrieren, indem mehrere Informatiksysteme in einem Verbund zusammengefasst werden. Dies hat den Vorteil, dass Grunddaten wie Personalien nicht für jedes Informationssystem separat eingegeben werden müssen; die Zugriffsberechtigung der angeschlossenen Stellen auf die einzelnen Daten wird dabei nicht erweitert. Datenabgleich und -weiterleitung erfolgen überdies zunehmend auf elektronischem Weg. Haben Behörden die Befugnis, in ihren Registern einen allgemein einsetzbaren Personenidentifikator systematisch zu verwenden, schafft dies eine technische Voraussetzung dafür, dass ein gesetzlich vorgesehener Datenaustausch in automatisierter und somit effizienter Form erfolgen kann.

Damit Behörden nicht in unrechtmässiger Weise Persönlichkeitsprofile bilden können, bedarf es präventiver Massnahmen. So ist generell darauf zu achten, dass Weiterleitung und Abgleich von Daten nur dort automatisiert werden sollen, wo dies erforderlich ist. Zudem obliegt es dem Gesetzgeber, diesbezüglich den dazu erfor-

derlichen Entscheid zu treffen. Es bedarf also einer ausdrücklichen gesetzlichen Grundlage, wonach der Datenaustausch anhand der AHVN und damit in automatisierter Form erfolgen kann.[18] Ein weiteres Instrument besteht darin, die Schnittstellen von IT-Systemen innerhalb der Verwaltung systematisch zu überwachen, wofür periodische Risikoanalysen durchgeführt werden müssen.

Höhere Informationssicherheit durch sektorielle Personenidentifikatoren?

Im bereits erwähnten Gutachten[19] erinnert der Experte daran, dass kein System absolut vor Angriffen geschützt werden könne. Er beschreibt zudem Möglichkeiten, wie den Verknüpfungsmöglichkeiten von Datenbanken mit personenbezogenen Daten (über Quasi-Identifikatoren oder die AHVN) grundsätzlich begegnet werden könnte. Sollen die Datenschutzbedenken grundsätzlich ausgeräumt werden, empfiehlt der Gutachter daher, die gesamte Datenbanklandschaft neu zu konzipieren. Personenidentifizierende Daten und Sachdaten müssten in getrennten Datenbanken gespeichert sein. Die personenidentifizierenden Daten müssten zudem redundanzfrei gehalten werden. Redundanz bei Informationen liegt vor, wenn Daten mit identischem Informationsgehalt mehrfach vorhanden sind. Identitätsmerkmale wie Name, Vorname oder AHVN einer Person dürften daher nur in einer einzigen Datenbank gespeichert werden. Die Verknüpfung der personenbezogenen Daten mit den Sachdaten dürfte ausschliesslich anhand von speziellen und geheimzuhaltenden Verknüpfungstabellen («Linkage Tables») möglich sein. Allein die Einführung von sektorspezifischen Identifikatoren, ohne die dargelegten Änderungen in der Systemarchitektur, sei hingegen nicht zielführend.

Verbesserungen des Datenschutzes bei der Verwendung von Personenidentifikationsnummern durch Kantone, Gemeinden und Dritte

Die vorstehenden Ausführungen zu den Personenidentifikatoren des Bundes im Allgemeinen und zur AHVN im Besonderen gelten sinngemäss auch für Personenidentifikatoren der Kantone. Es liegt jedoch in der Zuständigkeit der Kantone, die Zuordnung und systematische Verwendung derselben zu regeln. Beim Erlass der diesbezüglichen datenschutzrechtlichen Vorschriften haben sie den grundrechtlichen Anspruch auf Privatsphäre gemäss Artikel 13 Absatz 2 der Bundesverfassung (BV)[20] zu beachten. Der Gehalt dieser Bestimmung verpflichtet sie, alle erforderlichen Massnahmen zu treffen, um die Bürgerinnen und Bürger vor missbräuchlicher Verwendung ihrer persönlichen Daten zu schützen.

1.1.4 Exkurs: Nutzung der amerikanischen Sozialversicherungsnummer

Die ausgedehnte Nutzung der amerikanischen Sozialversicherungsnummer wird häufig thematisiert. In den USA ist die Verwendung der Social Security Number (SSN) durch Behörden und gleichermassen auch durch Private stark verbreitet. Dies

18 Vgl. Art. 32*a*bis Abs. 2 des Waffengesetzes vom 20. Juni 1997; SR **514.54.**
19 Vgl. Basin, a.a.O.
20 SR **101**

hat verschiedene Gründe. Einerseits fällt das offizielle Ausweis- und Registerwesen der USA in die Zuständigkeit der Bundesstaaten und ist daher in jedem Bundesstaat unterschiedlich geregelt. Diese Struktur reflektiert zugleich die Auffassungen betreffend Kompetenzen und Aufgaben des Staats schlechthin. In den USA wäre es undenkbar, ein zentrales Register einzuführen, das die Identitäts- und Zivilstandsdaten der gesamten Wohnbevölkerung speichert. Ein solches System, wie es in zahlreichen europäischen Staaten zum Standard gehört, gälte als übermässige staatliche Überwachung und fände insgesamt nicht die notwendige Akzeptanz. Unter diesen Umständen bildet die Social Security Card mit der aufgedruckten SSN das einzige landesweit einheitliche Identifikationsmittel, wobei grundsätzlich die gesamte Wohnbevölkerung über eine SSN verfügt. Diese Umstände führen dazu, dass oftmals die Social Security Card oder die SSN als Identifikationsmittel herangezogen werden. Auch zum Zweck der Authentifikation greift man in den USA regelmässig auf die SSN oder die Social Security Card zurück.

Anderseits sind in den USA auch Privatpersonen befugt, die SSN systematisch zu verwenden. Insbesondere die Betreiber der drei grossen «Bonitätsdatenbanken» bzw. «Kreditauskunfteien» arbeiten mit der SSN. Dasselbe gilt für Kreditkartenunternehmen, Banken, Leasing-Gesellschaften und dergleichen mehr, bei denen die Kreditauskunfteien regelmässig Informationen einholen. Anhand der SSN bilden sie aus diesen Informationen Persönlichkeitsprofile über die finanzielle Situation von bestimmten Einzelpersonen, um deren Kreditwürdigkeit zu bewerten. Das Risiko von Identitätsdiebstählen im Zusammenhang mit der SSN ist auch in diesem Kontext zu sehen. Wer eine fremde Identität vortäuscht, um an ein Kreditgeschäft zu kommen (vorzugsweise eine Identität mit hohem Bonitäts-Score), benötigt daher unter anderem auch Kenntnis von der SSN seines Opfers.

Diese Zusammenhänge gilt es bei der Vorlage zur erweiterten Verwendung der AHVN zu beachten. Dabei ist hervorzuheben, inwiefern sich die vorgesehene Regelung von der Situation in den USA unterscheidet: Auch künftig soll in der Schweiz eine Verwendung der AHVN durch Private ausgeschlossen sein. Zudem besteht in der Schweiz – im Unterschied zu den USA – ein landesweit einheitliches Ausweis- und Registerwesen. Damit ist sichergestellt, dass die Authentifikation auch künftig nur anhand amtlicher Ausweise erfolgen wird. Daten- oder Identitätsdiebstahl infolge weitreichender Verwendung der AHVN durch die Behörden von Bund, Kantonen und Gemeinden ist daher nicht zu befürchten.

1.2 Gewählte Lösung und geprüfte Alternativen

1.2.1 Gewählte Lösung: Systematische Verwendung der AHVN durch alle Behörden

Die systematische Verwendung der AHVN in einer Sammlung mit Personendaten führt zu einer eindeutigen Personenidentifikation und damit zu einer besseren Qualität des Datenbestands. Den allfälligen Risiken, die damit verbunden sind, kann mit tragbaren Massnahmen begegnet werden. Eine generelle Ermächtigung der Behörden von Bund, Kantonen und Gemeinden zur systematischen Verwendung der AHVN erweist sich hinsichtlich der Sachdienlichkeit, der Durchführbarkeit und der

Verhältnismässigkeit als ausgewogene Lösung. Im Einzelnen sind die nachfolgenden Punkte zu erwähnen:

Verhinderung von kostenintensiven Verwaltungsfehlern

Die wachsende Bevölkerung und die Zunahme der Aufgaben der öffentlichen Verwaltungen führen zu mehr Daten und Mutationen. Zudem nimmt die Zahl der komplexen Namen (beispielsweise Doppelnamen, Namen mit Sonderzeichen oder solche, die in die lateinische Schrift transkribiert werden müssen) zu. Eine manuelle Bearbeitung derselben ist zeitintensiv und auch fehleranfällig. Der Einsatz eines Personenidentifikators in Form einer Zahlenfolge hilft wesentlich, diese Probleme zu bewältigen. Dies gilt ganz besonders für den Einsatz der AHVN, zumal der von der ZAS sorgfältig gepflegte Personendatensatz der UPI-Datenbank sehr zuverlässig ist. Via entsprechende Meldung von ZEMIS und Infostar werden die Identifikationsattribute der in der UPI-Datenbank registrierten Personen ständig aktualisiert. Die hohe Datenqualität der UPI-Datenbank bietet dementsprechend Gewähr, dass eine Person korrekt identifiziert werden kann. Somit trägt die systematische Verwendung der AHVN im Rahmen der Datenbearbeitung wesentlich dazu bei, dass Verwechslungen von Personendaten vermieden werden.

Mehr Effizienz dank automatisiertem Datenaustausch zwischen den Behörden

Die systematische Verwendung eines eindeutigen Personenidentifikators ermöglicht einen medienbruchfreien Datenaustausch zwischen Behörden. Unter einem Medienbruch versteht man einen Wechsel des informationstragenden Mediums innerhalb eines Informationsverarbeitungsprozesses. Er unterbricht den Geschäftsablauf dadurch, dass Daten in einer anderen Form weitergereicht werden müssen, als sie empfangen wurden. Ein Medienbruch entsteht z. B., wenn elektronisch vorhandene Informationen auf Papier ausgedruckt und weiterverarbeitet werden, um dann von Hand wieder in einem anderen IKT-System erfasst zu werden. Wo der Gesetzgeber dies ausdrücklich erlaubt, kann die Datenkommunikation anhand der AHVN automatisiert erfolgen. Dadurch werden interne Prozesse und Querprozesse zwischen Behörden vereinfacht und die Kosteneffizienz gesteigert. Dies wiederum ermöglicht einen wirksamen und wirtschaftlichen Einsatz der öffentlichen Mittel, wie dies Artikel 43*a* Absatz 5 BV sowie Artikel 12 Absatz 4 zweiter Satz des Finanzhaushaltgesetzes vom 7. Oktober 2005[21] verlangen. Die öffentlichen Mittel werden auch insofern geschont, als der gesetzgeberische Aufwand für die Anpassung von Spezialgesetzen auf der Ebene von Bund, Kantonen und Gemeinden wegfällt.

Die vom Gesetzgeber vorgesehenen und damit rechtmässigen Datenverknüpfungen, beispielsweise zu statistischen Zwecken[22], führen ebenfalls zu genaueren Ergebnissen, wenn sie anhand eines eindeutigen Personenidentifikators durchgeführt werden können.

21 SR **611.0**

22 Die Verknüpfungen zu statistischen Zwecken erfolgen gestützt auf Art. 14*a* des Bundesstatistikgesetzes vom 9. Oktober 1992 (SR **431.01**), Art. 14 der Statistikerhebungsverordnung vom 30. Juni 1993 (SR **431.012.1**) und die Datenverknüpfungsverordnung vom 17. Dezember 2013 (SR **431.012.13**).

Vermeidung von Verwechslungen

Für die einzelnen Bürgerinnen und Bürger – insbesondere für jene mit stark verbreiteten Namen – bringt die systematische Verwendung der AHVN ebenfalls einen Mehrwert: Jede Person, deren Personendaten gesammelt werden, hat Anspruch darauf, dass die darauf gestützten Verwaltungsabläufe abgewickelt werden, ohne dass es zu Verwechslungen mit anderen registrierten Personen kommt. Für die Betroffenen können Verwechslungen erhebliche Unannehmlichkeiten zur Folge haben. Die Verwechslungen ergeben sich in der Regel aus Unvollständigkeiten bei der Registerführung, aus Rechtschreibfehlern oder aus dem Umstand, dass ein Name oder eine Kombination von Namen stark verbreitet ist. So lauten insgesamt rund 950 aller rund 2 330 700 im offiziellen Telefonbuch der Schweiz eingetragenen privaten Telefonanschlüsse auf Peter Müller. Werden die Personen zusätzlich anhand eines eindeutigen Personenidentifikators in einer Datenbank registriert, ist die Verwechslungsgefahr beseitigt. Die insofern erhöhte Qualität des Datenbestands in den Benutzerregistern dient der Datenrichtigkeit und damit einem wichtigen Aspekt des Persönlichkeitsschutzes im Umgang mit Personendaten (vgl. Ziff. 1.1.3).

Sektorielle Nummern bleiben möglich

Die Vorlage belässt die Möglichkeit, für bestimmte Register die systematische Verwendung der AHVN im Spezialgesetz zu untersagen; dies, um für Bereiche mit besonders sensiblen Daten jegliches Restrisiko betreffend unerlaubte Profilbildungen ausschliessen zu können.

Begleitmassnahmen und regelmässige Risikoanalysen

Zur Einhaltung der Begleitmassnahmen müssen die Verwenderinnen und Verwendern der AHVN ihre Informationssysteme auf dem neusten Stand halten. Somit dient der vorliegende Gesetzesentwurf auch der generellen Erhöhung der Informationssicherheit in der öffentlichen Verwaltung. Werden die Risikoanalysen regelmässig durchgeführt und die Begleitmassnahmen konsequent umgesetzt, gefährdet die systematische Verwendung der AHVN weder den Datenschutz noch führt sie zum «gläsernen Bürger».

1.2.2 Geprüfte Alternativen

Bewilligungsverfahren

Nach einem System mit einer Bewilligungspflicht würde die Befugnis zur systematischen Verwendung der AHVN nicht durch den Gesetzgeber, sondern durch Verfügung einer Bewilligungsbehörde erteilt. Diese hätte in jedem Einzelfall zu prüfen, ob die Behörde, die ein Gesuch auf systematische Verwendung der AHVN stellt, den Datenschutz und die Informationssicherheit gewährleisten kann. Die gesuchstellende Behörde hätte insbesondere zu belegen, dass sie in der Lage ist, die erforderlichen Massnahmen technischer und organisatorischer Art einzuhalten. Die Bewilligungsbehörde hätte zudem anhand von periodischen Stichprobenkontrollen bei den Inhabern der Bewilligung zu prüfen, ob diese die Bewilligungsvoraussetzungen weiterhin erfüllen und ob sie die Sorgfalts- und Mitwirkungspflichten einhalten. Ein

solches System liesse sich indessen nur mit einem Ausbau des Verwaltungsaufwands und insbesondere mit hohen Kosten einrichten, dem kein angemessener zusätzlicher Nutzen gegenüberstünde, zumal die IT-Systeme naturgemäss stetem Wandel unterstehen und die Erteilung der Bewilligung jeweils nur aufgrund einer Momentaufnahme zum Bewilligungszeitpunkt erfolgen könnte. Mit Blick darauf, dass den Behörden von Bund, Kantonen und Gemeinden zudem eine hohe Gesetzestreue attestiert wird, ist auf aufwendige Kontroll- und Überwachungsmechanismen zu verzichten und stattdessen auf den Grundsatz der Selbstkontrolle zu setzen.

Sektorielle Nummern

Ein System mit sektoriellen Personenidentifikatoren wurde ebenfalls geprüft. Dabei werden jeder zu verzeichnenden natürlichen Person mehrere Identifikatoren zugewiesen. Diese werden jeweils ausschliesslich für die jeweilige Verwaltungstätigkeit im betreffenden Sektor der Verwaltung, z. B. in einem Steuersektor oder in einem Sozialversicherungssektor, verwendet. Damit dennoch eine effiziente elektronische Kommunikation zwischen zwei Verwaltungsstellen in verschiedenen Sektoren stattfinden kann, wird ein zentraler Identifikations- und Kommunikationsserver benötigt. Solche Verwaltungssektoren existieren in der heutigen Verwaltungsstruktur jedoch nicht, müssten also zuerst geschaffen werden. Anlässlich der Vernehmlassung zum Entwurf zum Bundesgesetz über die sektoriellen Personenidentifikatoren im Jahr 2004 erachteten die meisten Kantone und Organisationen im Bereich des E-Government und der E-Administration, die Sektorialisierung sei zu komplex und zu kostspielig, zudem fehleranfällig und bilde daher eine in der Praxis kaum praktikable Lösung.

Auch aus heutiger Sicht wäre eine generelle Einführung von sektoriellen oder anderen, alternativen Personenidentifikatoren für zahlreiche Behörden von Bund, Kantonen und Gemeinden nicht wünschenswert, da sie zu kostspielig wäre und gar nicht zur Risikominderung beitragen würde. Teilweise würde die Einführung eines solchen Systems sogar einen Rückschritt bedeuten, zumal im Vertrauen auf die Beibehaltung der aktuellen Regelung (mit der AHVN als einem eindeutigen Personenidentifikator für Behörden) bereits Dispositionen getroffen und Investitionen getätigt worden sind. Unter diesen Umständen ist die Einführung eines umfassenden Systems mit sektoriellen Personenidentifikatoren nicht zu befürworten. Falls in einem bestimmten Bereich die Verwendung eines besonderen Personenidentifikators gewünscht wird, bleibt dies allerdings auch mit dem vorliegenden Entwurf möglich.

1.3 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrats

1.3.1 Verhältnis zur Legislaturplanung

Die Vorlage ist weder in der Botschaft vom 27. Januar 2016[23] zur Legislaturplanung 2015–2019 noch im Bundesbeschluss vom 14. Juni 2016[24] über die Legislaturpla-

23 BBl **2016** 1105
24 BBl **2016** 5183

nung 2015–2019 angekündigt. Sie trägt aber dazu bei, die «E-Government-Strategie Schweiz» umzusetzen (vgl. Ziff. 4.2). Die «E-Government-Strategie Schweiz» ist ein Geschäft der Legislaturplanung 2015-2019.

1.3.2 Verhältnis zu Strategien des Bundesrates

Die vom Bundesrat verabschiedete «E-Government-Strategie Schweiz»[25] verfolgt das Ziel, Wirtschaft und Bevölkerung von besseren Dienstleistungen und einer effizienteren Verwaltung profitieren zu lassen. Das Umsetzungsinstrument der aktuellen «E-Government-Strategie Schweiz» ist der Schwerpunktplan 2017–2019[26]. Dieser enthält elf operative Ziele. Das operative Ziel Nr. 7 lautet: «Die Zuordnung von Daten zu einer bestimmten Person im elektronischen Austausch zwischen Informationssystemen ist bis 2019 sichergestellt.» Weiter wird ausgeführt, ein eindeutiges Personenkennzeichen, das in allen Fachbereichen und auf allen Staatsebenen angewendet werden könne, habe bisher noch nicht etabliert werden können. Daher bestehe hierin grosser Handlungsbedarf. Insofern trägt diese Vorlage dazu bei, die «E-Government-Strategie Schweiz» umzusetzen.

Der erwähnte Schwerpunktplan sieht ferner die Einführung einer E-ID vor (operatives Ziel Nr. 5). Gesicherte Identitäten sind die Basis für Rechtssicherheit. Der vom Bundesrat verabschiedete Entwurf für ein neues Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID) bezweckt, den sicheren elektronischen Geschäftsverkehr zwischen Privaten und Behörden oder unter Privaten zu fördern.[27] Damit auch anspruchsvollere Geschäftsprozesse online abgewickelt werden können, müssen die Vertragspartner Vertrauen in die Identität des Gegenübers haben können. Diesem Bedarf soll in der Schweiz mit der Schaffung von anerkannten elektronischen Identifizierungseinheiten für natürliche Personen nachgekommen werden. Eine von der AHV unabhängige E-ID-Registrierungsnummer dient zur Verbindung der betreffenden Person mit der ausgegebenen E-ID.

Das E-ID-Konzept geht von einer Aufgabenteilung zwischen Staat und Privaten aus: Der Bund gibt keine eigene E-ID heraus, sondern kann E-ID von privaten Anbietern (wie die SuisseID der Post) staatlich anerkennen, wenn diese die gesetzlichen Anforderungen erfüllen. Durch die Anerkennung wird den Anbietern von Identitätsdienstleistungen (Identity Provider, IdP) erlaubt, staatlich geführte und bestätigte Personenidentifizierungsdaten für die Erbringung ihrer Dienstleistungen zu verwenden. Den IdP soll deshalb erlaubt werden, die AHVN – ausschliesslich – zu diesem eingeschränkten Zweck systematisch zu verwenden. Im Übrigen sollen sie die AHVN nur den Betreiberinnen eines E-ID-verwendenden Dienstes bekannt geben dürfen, die selbst zur systematischen Verwendung der AHVN berechtigt sind. Der Umstand, dass die IdP weder Behörden sind noch eine öffentliche Aufgabe im engeren Sinn erfüllen, soll der umschriebenen systematischen Verwendung der

25 Die Strategie ist im Internet unter folgender Adresse abrufbar: www.egovernment.ch/de/umsetzung/e-government-strategie/
26 Der Schwerpunktplan ist im Internet unter folgender Adresse abrufbar: www.egovernment.ch/de/umsetzung/schwerpunktplan1
27 BBl **2018** 3915 3989

AHVN durch die IdP nicht entgegenstehen. Die angestrebte Einführung einer E-ID in der dargelegten Form wird durch das vorliegende Gesetzgebungsprojekt somit nicht gefährdet.

1.4 Erledigung parlamentarischer Vorstösse

Die im Postulat 17.3968 «Sicherheitskonzept für Personenidentifikatoren» verlangte Risikoanalyse erfolgt im Rahmen dieser Botschaft unter Ziffer 1.1.3. Das Postulat wird zur Abschreibung beantragt.

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

2.1 Stellungnahme der Eidgenössischen AHV/IV-Kommission

Die AHV/IV-Kommission ist grundsätzlich mit einer generellen Erweiterung der systematischen Verwendung der AHVN durch Behörden von Bund, Kantonen und Gemeinden für die Erfüllung ihrer gesetzlichen Aufgaben einverstanden. Sie legt allerdings Wert auf die Feststellung, dass die neue Regelung möglichst transparent ausgestaltet sein sollte.

2.2 Vernehmlassungsverfahren

Der Bundesrat hat das EDI am 7. November 2018 damit beauftragt, eine Vernehmlassung zum Vorentwurf der AHVG-Änderung durchzuführen. In einem Brief gleichen Datums lud das EDI die Kantone, die in der Bundesversammlung vertretenen politischen Parteien, die Dachorganisationen der Wirtschaft sowie weitere Verbände und Organisationen ein, sich bis am 22. Februar 2019 zum Vorentwurf zu äussern. Eine ausführliche Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens ist im Vernehmlassungsbericht zu finden.[28]

Im Grundsatz begrüsste ein Grossteil der Vernehmlassungsteilnehmenden die Einführung einer generellen Erlaubnisnorm zugunsten von Behörden. In einzelnen Punkten waren die Teilnehmenden jedoch gespalten. Etliche wandten sich gegen die Regelung von technischen und organisatorischen Massnahmen auf der Gesetzesebene. Auch die vorgesehene Bestimmung zur Risikoanalyse wurde von einigen Teilnehmenden für überflüssig gehalten, zumal es bereits im Rahmen der bestehenden Datenschutzkonzepte vorgesehen sei, allfällige Verknüpfungsrisiken zu beachten. Nahezu einhellig lehnten die Teilnehmenden es ab, die Strafbestimmung zu den technischen und organisatorischen Massnahmen zu verschärfen, da dies zu unlösbaren Abgrenzungsfragen führen würde. Nach der Vernehmlassung wurde der Vor-

28 www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2019 > EDI

entwurf insofern geändert, als auf die ursprünglich vorgesehene Verschärfung der Strafbestimmung verzichtet wurde. Im Übrigen unterscheidet sich der Entwurf nur in einigen wenigen, redaktionellen Punkten vom Vorentwurf.

3 Rechtsvergleich

Ein Blick auf die Rechtsordnung anderer Staaten zeigt, dass Personenidentifikatoren sehr unterschiedlich geregelt werden können. Während im österreichischen System aus der jeweiligen Stammzahl einer Person jeweils ein bereichsspezifisches Personenkennzeichen abgeleitet wird, kennen Schweden und andere skandinavische Länder einen einheitlichen Personenidentifikator, der für sämtliche Lebensbereiche öffentlicher und privater Natur anwendbar ist. Die ausgedehnte Nutzung der amerikanischen Sozialversicherungsnummer geht wiederum darauf zurück, dass sie die einzige landesweit einheitliche Identifikationsnummer darstellt (vgl. Ziff. 1.1.4).

4 Grundzüge der Vorlage

4.1 Die beantragte Neuregelung

Die Behörden des Bundes, der Kantone und der Gemeinden sollen für die Erfüllung ihrer gesetzlichen Aufgaben die AHVN systematisch ohne spezialgesetzliche Grundlage verwenden dürfen. Die Berechtigung zur systematischen Verwendung soll sich bereits aus der betreffenden Bestimmung des AHVG ergeben, es soll mithin eine generelle Erlaubnisnorm für Behörden geschaffen werden. Damit braucht es in Zukunft grundsätzlich keine spezialgesetzliche Erlaubnisnorm für jeden einzelnen Verwendungszweck und jeden einzelnen Verwender. Der Gesetzgeber behält jedoch die Möglichkeit, bereichsspezifische Personenidentifikatoren zu schaffen und für den betreffenden Bereich den systematischen Gebrauch der AHVN zu untersagen.

Einrichtungen ohne Behördencharakter, die mit der Erfüllung einer Verwaltungsaufgabe betraut sind, sollen wie bisher nur aufgrund einer spezialgesetzlichen Grundlage zur systematischen Verwendung der AHVN ermächtigt sein. Die nach dem aktuellen Recht bereits bestehenden spezialgesetzlichen Berechtigungen zur systematischen Verwendung der AHVN werden beibehalten. Ein Teil der betreffenden Bestimmungen wird allerdings redaktionell angepasst. Die Berechtigung zur systematischen Verwendung durch Bildungsinstitutionen ist – wie im geltenden Recht – bereits auf der Stufe des AHV-Rechts verankert, wobei die neue Regelung sämtliche Bildungsinstitutionen erfasst. Diese haben sowohl sozialversicherungsrechtliche Pflichten als auch Aufgaben der Bundesstatistik zu erfüllen. Die systematische Verwendung rein privater Art soll weiterhin ausgeschlossen sein. Ferner sollen die sichernden Massnahmen einen hinreichenden Stellenwert erhalten (vgl. dazu im Einzelnen die Ausführungen unter Ziff. 4.2).

4.2 Begleitmassnahmen

Bereits nach geltendem Recht gibt es Vorgaben betreffend organisatorische, personelle, infrastrukturelle und technische Sicherheitsmassnahmen. Sie sind in einer Departementsverordnung enthalten.[29] Die grundlegenden Prinzipien sollen künftig auf Gesetzesstufe geregelt werden. Es handelt sich um die Regelung von Verantwortlichkeiten, Schulung und Dokumentation bezüglich IT-Sicherheit und um Massnahmen, die darauf abzielen, die Zugriffsrisiken zu verkleinern (vgl. dazu Risikoanalyse, Ziff. 1.1.3). Neu wird verlangt, dass ein ISDS erstellen muss, wer die AHVN systematisch verwendet. Ebenfalls neu ist die Vorgabe, dass Bund und Kantone Risikoanalysen durchzuführen haben, deren Zweck darin besteht, die Risiken von unerlaubten Zusammenführungen von Datenbanken – insbesondere anhand von Schnittstellen – zu erkennen und zu verhindern. Sie stützen sich dabei auf Verzeichnisse, welche die Datenbanken auflisten, in denen die AHVN systematisch verwendet wird.

Die Vorlage ändert nichts an den bereits bestehenden Bestimmungen zum Datenaustausch. Ebenso wenig werden neue Zugriffsrechte erteilt. Es erfolgt also keine Erweiterung der bestehenden Einsichts-, Bekanntgabe- und Bearbeitungsrechte. Soll ein Datenaustausch zwischen den Behörden anhand der AHVN stattfinden, bedarf es dazu einer ausdrücklichen gesetzlichen Grundlage.

Die bereits bestehenden strafrechtlichen Regelungen bleiben inhaltlich unverändert: Wer die AHVN systematisch verwendet, ohne dazu berechtigt zu sein, wird wie bisher mit Geldstrafe bestraft. Wird unterlassen, technische und organisatorische Massnahmen zu treffen, gilt dies weiterhin als Übertretung. Sie wird mit Busse bestraft.

4.3 Keine Pflicht zur Neukonzeption der Datenbankarchitektur

Aus dem bereits erwähnten Gutachten[30] geht hervor, dass die Datensätze von verschiedenen Datenbanken auch mit den Quasi-Identifikatoren Namen, Vornamen und Geburtsdatum mit einer Genauigkeit von 99,98 Prozent verknüpfbar sind. Der Präzisionszuwachs, den die systematische Verwendung der AHVN liefere, sei damit für den Datenschutz nicht entscheidend. Die grundsätzlichen datenschutzrechtlichen Probleme würden mithin auch nicht durch das Einführen von sektorspezifischen Nummern gelöst. Vielmehr seien sie regelmässig in der Datenbankarchitektur angelegt, indem sowohl Personen- als auch Sachdaten jeweils in derselben Datenbank gespeichert würden. Unter dem Aspekt des Informationsschutzes wäre ein Informatiksystem jedoch idealerweise so ausgestaltet, dass die personenbezogenen Daten redundanzfrei gehalten und in einer eigenen Datenbank gespeichert würden, die von den jeweiligen Sachdaten getrennt sei. Attribute wie Name, Vorname, Geburtsdatum

29 Verordnung des EDI vom 7. November 2007 über die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der AHV-Versichertennummer ausserhalb der AHV (SR **831.101.4**).

30 Vgl. Basin, a.a.O.

oder AHVN dürften ausschliesslich in einer einzigen Datenbank registriert sein. Die Verbindung von Personendaten mit den entsprechenden Sachdaten wäre ausschliesslich mithilfe von speziellen und geheimzuhaltenden Verknüpfungstabellen («Linkage Tables») möglich.

Bei einer solchen Neukonzeption der Systemarchitektur wäre der Datenaustausch zwar grundsätzlich nicht in Frage gestellt. Die Attribute könnten aber nicht mehr dezentral abgespeichert werden. Man müsste daher immer über die zentral gehaltene Datenbank, die diese Attribute enthielte, auf die Daten zugreifen. Dadurch würden der Netzverkehr und die Zugriffe auf diese Datenbanken zunehmen, was wiederum die Fehleranfälligkeit ansteigen liesse. Die Datenbanken würden «Bottle Necks» und kritische Systeme darstellen, die permanent verfügbar gehalten werden müssten. Dies zu konzipieren und umzusetzen wäre sehr aufwendig und würde bei Bund, Kantonen und Gemeinden sehr hohe Kosten verursachen. Die Erfahrungen mit dem Jahr-2000-Problem haben gezeigt, dass bereits kleine Änderungen in Datenformaten und in der Art und Weise, wie die Daten gespeichert und verarbeitet werden, sehr hohe Kosten verursachen können. Zudem würde die Beseitigung von Redundanz auch zu Schwierigkeiten im operativen Betrieb der entsprechenden Datenbanken führen: Ohne Redundanz wäre es schwieriger, allfällige Fehler bei der Eingabe oder Verarbeitung von Daten durch die Benutzerinnen und Benutzer zu erkennen und zu korrigieren. Zudem ist es bei Datenverlust nicht mehr möglich, auf redundante Kopien zuzugreifen. Sind die Redundanzen beseitigt, ist man daher bei Datenverlusten noch stärker als üblich auf Backups angewiesen. Darüber hinaus wären Konsistenzprüfungen schwierig, weil kein Abgleich mit anderen (redundanten) Datenbanken erfolgen kann.

Eine Vorgabe, wonach eine Architektur mit getrennter Datenhaltung flächendeckend umzusetzen sei, hätte folglich zahlreiche Nachteile und hohe Kosten zur Folge. Zwar kann es in bestimmten Einzelfällen durchaus sinnvoll sein, bei geschlossenen Anwendungskreisen – wie z. B. im Gesundheitswesen – eine Datenbankarchitektur mit minimaler Datenhaltung einzurichten, wenn neue Datenbanken erstellt werden. Dies ist allerdings nur sinnvoll, wenn eine solche Struktur für einen grossen Anwendungskreis integral neu eingeführt werden kann. In der Regel werden jedoch nur einzelne Datenbanken neu geschaffen oder es werden in bestehenden Datenbanken neue Attribute ergänzt. Aus diesen Gründen – operative Schwierigkeiten und geringer Mehrwert, zugleich aber hohe Kosten – werden die Verwender der AHVN nicht gesetzlich verpflichtet, ihre Datenbankarchitektur von Grund auf zu überarbeiten. Es bleibt ihnen allerdings unbenommen, eine getrennte Datenhaltung einzurichten, falls sie dies für nützlich und machbar erachten.

4.4 Unveränderte Bestimmungen über Schweigepflicht der Behörden und Datenbekanntgabe

Das schweizerische öffentliche Recht sieht im Grundsatz vor, dass Behörden die Personendaten, über die sie verfügen, geheimzuhalten haben. Ausnahmen vom Amtsgeheimnis bestehen nur, wenn eine gesetzliche Bestimmung besteht, die den Behörden die Datenbekanntgabe an andere Behörden oder den Abgleich von perso-

nenbezogenen Daten zwischen den Behörden ausdrücklich erlaubt. Die Vorlage zur erweiterten systematischen Verwendung der AHVN tastet diese Grundsätze nicht an. Ebenso wenig schafft sie neue gesetzliche Grundlagen zur Erhebung von Daten oder zur Datenbekanntgabe. Wo das Gesetz die Bekanntgabe von Daten unter Verwendung von Schnittstellen erlaubt, darf die AHVN überdies als zusätzliche Information nur ausgetauscht werden, wenn für einen solchen Datenaustausch mittels AHVN eine formell-gesetzliche Grundlage besteht. Bereits im geltenden Recht gibt es vereinzelt Bereiche, die dies vorsehen, so beispielsweise Artikel 32*a*bis des Waffengesetzes vom 20. Juni 1997. Auch die Zahl der gesetzlich zulässigen Datenverknüpfungen wird durch die vorgeschlagene Neuregelung der systematischen Verwendung der AHVN nicht ausgeweitet. Verknüpfungen sind nach wie vor nur mit einer formell-gesetzlichen Grundlage zulässig, wie sie beispielsweise im Bundesstatistikgesetz oder im Volkszählungsgesetz[31] enthalten sind.

4.5 Abstimmung von Aufgaben und Finanzen

Für die Finanzierung der erweiterten Verwendung der AHVN ausserhalb der AHV können Gebühren erhoben werden, um die bescheidenen Kosten zu decken. Eine detaillierte Beschreibung möglicher Auswirkungen des Entwurfs findet sich unter den Ziffern 6.1 und 6.2.

4.6 Umsetzungsfragen

Wie bisher soll die ZAS für die systematische Verwendung der AHVN Gebühren erheben können. Die Einzelheiten werden auf Verordnungsebene geregelt. Ausnahmen von der Gebührenpflicht sollen auch künftig möglich sein. Denkbar sind auch pauschale Abgeltungen durch die Kantone nach Massgabe der Nutzungsfrequenz.

Die Risikoanalyse, welche die Einheiten von Bund und Kantonen gemäss Artikel 153*e* Absatz 1 E-AHVG regelmässig durchzuführen haben, können im Rahmen der bereits für den Datenschutz vorgesehenen Kontrollen durchgeführt werden. Als zusätzlicher Punkt ist aber die systematische Verwendung der AHVN zu berücksichtigen. Die Verzeichnisse gemäss Artikel 153*e* Absatz 2 E-AHVG zu führen, die für die Risikoanalyse beizuziehen sind, obliegt auf der Ebene des Bundes den Departementen. Kantone und Gemeinden bestimmen die Zuständigkeit zur Führung der Verzeichnisse in eigener Kompetenz.

Die Begleitmassnahmen, die bei der systematischen Verwendung einzuhalten sind, sind aktuell in der Verordnung des EDI enthalten. Künftig sollen die Grundsätze auf der Gesetzesstufe stehen.

31 SR **431.112**

5 Erläuterungen zu einzelnen Artikeln

5.1 Bundesgesetz über die Alters- und Hinterlassenenversicherung

Art. 49a Bst. g

Mit der Zuweisung einer AHVN erfolgt eine Eintragung in das zentrale Register nach Artikel 71 Absatz 4 Buchstabe a AHVG. Es kann nicht systematisch daraus abgeleitet werden, dass die Person in der AHV versichert ist. Deshalb wird der Begriff «Versichertennummer» durch «AHV-Nummer» ersetzt.

Im Übrigen ist darauf hinzuweisen, dass im Rahmen der Totalrevision[32] des Datenschutzgesetzes vom 19. Juni 1992[33] (DSG) der Begriff «Persönlichkeitsprofil» aufgehoben werden soll. Am Ende der parlamentarischen Beratungen wird darauf zu achten sein, dass die beiden Geschäfte koordiniert werden und allenfalls der Einleitungssatz in diesem Sinne geändert wird.

Art. 50d–50g

Diese Bestimmungen werden aufgehoben, weil die Regelung der systematischen Verwendung der AHVN ausserhalb der AHV in einen neu zu schaffenden 4. Teil des AHVG überführt wird.

Art. 87 achtes Lemma und Art. 88 viertes Lemma

Diese Bestimmungen werden aufgehoben, weil die Strafbestimmungen im 4. Teil des AHVG enthalten sein werden.

Art. 89

Die solidarische Haftung der Unternehmen widerspricht dem strafrechtlichen Grundsatz, wonach die Busse höchstpersönlich ist und nicht übertragen werden kann. Sie stellt somit eine versteckte Form der strafrechtlichen Verantwortlichkeit des Unternehmens dar. Artikel 79 des Bundesgesetzes vom 6. Oktober 2000[34] über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG), der für den ersten Teil des AHVG gilt (Art. 1 Abs. 1 AHVG), verweist namentlich auf Artikel 6 des Bundesgesetzes vom 22. März 1974[35] über das Verwaltungsstrafrecht, der auf die Widerhandlungen in Geschäftsbetrieben anwendbar ist. Artikel 89 kann daher bei dieser Gelegenheit aufgehoben werden.

32 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 6941.
33 SR **235.1**
34 SR **830.1**
35 SR **313.0**

Gliederungstitel nach Art. 153a

Vierter Teil: Systematische Verwendung der AHVN ausserhalb der AHV

Die geltenden Regelungen der vorliegenden Materie sind im ersten Teil (Die Versicherung) vierter Abschnitt (Die Organisation) platziert. Aus gesetzessystematischer Sicht ist dies ungünstig, geht es doch gerade nicht um die AHV und deren Organisation, sondern um die Verwendung der AHVN in Bereichen ausserhalb der AHV. Im Interesse der Transparenz der Rechtsetzung und der Auffindbarkeit von rechtlichen Regelungen soll die systematische Verwendung der AHVN als Personenidentifikator ausserhalb der AHV in einem eigenen Teil des AHVG geregelt werden. Direkt vor den Schlussbestimmungen wird daher ein neuer, vierter Teil eingefügt (Art. 153*b* ff.), der Bestimmungen über die systematische Verwendung der AHVN als Personenidentifikator ausserhalb der AHV enthält.

Art. 153b Begriff

Die Bestimmung enthält die Legaldefinition der systematischen Verwendung, die bisher in Artikel 134bis der Verordnung vom 31. Oktober 1947[36] über die Alters- und Hinterlassenenversicherung (AHVV) enthalten war. Angesichts von deren Bedeutung rechtfertigt es sich, sie neu ins Gesetz aufzunehmen. Inhaltlich bleibt die Regelung unverändert. Die Verwendung gilt als «systematisch», wenn die Nummer mit Personendaten verbunden wird und die Verwendung eine klar definierte Gruppe natürlicher Personen betrifft. Entscheidendes Kriterium soll sein, ob der essenzielle, kennzeichnende Teil der AHVN Eingang in eine Datensammlung findet und darin dauerhaft gespeichert wird. Dadurch kann vermieden werden, dass durch systematische Modifizierungen der vollständigen Nummern nach eigenem System (z. B. durch Weglassung des Ländercodes 756 in den ersten drei Stellen der 13-stelligen Nummer, durch Ergänzungen der Nummer mit einem Buchstaben bzw. einer weiteren Ziffer oder durch eine Verschlüsselung) die vom Gesetzgeber gewollte Kontrolle des Gebrauchs unterlaufen wird.

Art. 153c Berechtigte

Absatz 1: Dieser Absatz regelt, wer als Berechtigte in Frage kommt.

Buchstabe a Ziffern 1 und 2: Diese Ziffern beziehen sich auf die Bundesebene. Die Formulierung orientiert sich an der Struktur von Artikel 2 Absätze 1–3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG)[37]. Dieses unterscheidet zwischen Einheiten der zentralisierten und solchen der dezentralisierten Bundesverwaltung.

Ziffer 3: Auf Kantons- und Gemeindeebene ist ebenfalls massgebend, ob eine Einheit zur Verwaltung gehört. Interkantonale oder überkommunale Einheiten sind ausserhalb der Verwaltung angesiedelt. Soll ihnen die systematische Verwendung der AHVN ermöglicht werden, muss in den interkantonalen oder –kommunalen

36 SR **831.101**
37 SR **172.010**

Vertrag, der die betreffende Einheit begründet, eine entsprechende Grundlage gemäss Ziffer 4 aufgenommen werden (vgl. unten, Ziff. 4).

Ziffer 4: Sie erfasst die Personen und Organisationen des öffentlichen oder privaten Rechts, die eine Verwaltungsaufgabe erfüllen, aber weder der zentralen noch der dezentralen Verwaltung angehören. Sollen sie die Verwaltungsaufgabe, mit der sie betraut sind, unter systematischer Verwendung der AHVN erfüllen können, benötigen sie eine entsprechende Berechtigung im jeweiligen Spezialgesetz. Als konkretes Beispiel dienen die anerkannten Anbieter der obligatorischen Krankenpflege- und der obligatorischen Unfallversicherung. Sie gehören weder auf der Ebene des Bundes noch auf jener der Kantone zur Verwaltung, sind aber gesetzlich mit der Durchführung der genannten Sozialversicherungen betraut. Dafür sollen sie auch künftig zur systematischen Verwendung der AHVN berechtigt sein. Die entsprechenden spezialgesetzlichen Grundlagen bestehen bereits. Dasselbe gilt analog für die Durchführung der beruflichen Vorsorge. Die Vorsorgeeinrichtungen dürfen die AHVN ebenfalls – wie bisher – systematisch verwenden. Die bereits bestehenden diesbezüglichen Bestimmungen bleiben unverändert.

Ziffer 5: Bisher waren die kantonalen Bildungsanstalten gestützt auf Artikel 50*e* Absatz 2 Buchstabe d AHVG zur systematischen Verwendung der AHVN befugt. Diese Möglichkeit müssen sie auch künftig haben, denn einerseits fungieren sie als Hilfsorgane der AHV. Studierende der Hochschulen und auch Schülerinnen und Schüler der Sekundarstufe II (duale Berufsbildung oder berufliche Vollzeitausbildung) und der nichthochschulischen Tertiärstufe (höhere Berufsbildung) sind AHV-beitragspflichtig. In ihrer Rolle als Hilfsorgane der AHV nehmen die betreffenden Bildungsinstitutionen die notwendigen Meldungen für die Studierenden an die Ausgleichskassen vor und übernehmen gegebenenfalls das Inkasso für die Beiträge (Art. 29bis und 29ter AHVV). Für die korrekte Verbuchung der Beitragszahlung zugunsten der Betroffenen muss bei der Datenübermittlung die AHVN verwendet werden. Ausserdem verwenden Schulen mit besonderem Lehrplan (Sonderschulen) die AHVN im Rahmen der Invalidenversicherung. Schliesslich gibt es Kantone, in denen die Unfallversicherung für die Schülerinnen und Schüler via Schulen erfolgt.

Anderseits haben die Bildungsinstitutionen auch Aufgaben im Bereich der Bildungsstatistik zu erfüllen, also Aufgaben ausserhalb der AHV. Diese Erhebungen erfolgen ebenfalls unter Verwendung der AHVN. Unter diesen Umständen ist es ist sinnvoll, auch künftig sowohl den kantonalen Bildungsinstitutionen als auch jenen des Bundes für die Erfüllung ihrer bildungsstatistischen Aufgaben die systematische Verwendung der AHVN zu erlauben.

Buchstabe b: Im Unterschied zur Durchführung der sozialen Krankenversicherung und der obligatorischen Unfallversicherung ist die Durchführung von privatrechtlich geregelten Zusatzversicherungen keine Verwaltungsaufgabe. Es bestehen jedoch zahlreiche Verbindungen zwischen den Zusatzversicherungen auf der einen und der obligatorischen Unfall- bzw. Krankenversicherung auf der anderen Seite. Die Durchführung der Bereiche kann deshalb nicht isoliert betrachtet werden. Aus diesem Grund ermächtigt Artikel 47*a* des Versicherungsvertragsgesetzes vom 2. April 1908[38] die Anbieter von Zusatzversicherungen bereits nach geltendem

38 SR **221.229.1**

Recht zur systematischen Verwendung der AHVN. Dies soll auch künftig so bleiben. Bei dieser Regelung handelt es sich insofern um eine Ausnahme, als sie Privaten ermöglicht, für die Durchführung einer privatrechtlich geregelten Tätigkeit die AHVN systematisch zu verwenden.

Im Übrigen soll die AHVN auch weiterhin nicht zu rein privaten Zwecken verwendet werden dürfen. Dies gilt auch im Fall, dass sich die betroffenen Personen mit der systematischen Verwendung ihrer AHVN durch Private einverstanden erklären. Das Verbot rechtfertigt sich: Die ZAS kann die Datenabgleiche und Korrekturen im Interesse der Datenqualität gemäss Artikel 153*f* Buchstaben b und c gegenüber Privaten nicht gleichermassen durchsetzen. Vor allem aber dürfte das Risiko von unzulässigen Datenverknüpfungen bei einer systematischen Verwendung durch Private deutlich höher sein als bei einer Nutzung durch Behörden. Dasselbe gilt für das Risiko von unbefugten Zugriffen auf die Datensammlungen von Privaten. Aus Sicht des Datenschutzes und der Informationssicherheit ist eine Verwendung durch Private deshalb abzulehnen.

Absatz 2: Der Gesetzgeber soll weiterhin für bestimmte Bereiche anstelle der AHVN weitere Personenidentifikatoren vorsehen können. Er wird daher auch künftig die Möglichkeit haben, die systematische Verwendung der AHVN für einzelne Gebiete auszuschliessen. Zu denken ist an Bereiche, in denen besonders schützenswerte Personendaten im Sinne von Artikel 3 Buchstabe c DSG betroffen sind. Es sind dies Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer ethnischen Gruppe, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen.

Art. 153d Technische und organisatorische Massnahmen

Die zur systematischen Verwendung der AHVN berechtigten Behörden, Organisationen und Personen müssen die nötigen technischen und organisatorischen Massnahmen ergreifen, um einer missbräuchlichen Nutzung vorzubeugen. Dies dient der Wahrung der Informationssicherheit und des Datenschutzes. Dieser Artikel fasst die Pflichten zusammen, die bisher zum Teil in der Verordnung des EDI über die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der AHVN ausserhalb der AHV enthalten waren. Sie werden neu ins Gesetz aufgenommen und aktualisiert.

Die Sorgfaltspflichten bezwecken den Schutz vor missbräuchlicher Verwendung der AHVN. Die zur systematischen Verwendung der AHVN berechtigten Behörden, Organisationen und Personen sorgen fortlaufend dafür, dass die anwendbaren Sicherheitsstandards aufrechterhalten bleiben. Die Systeme müssen zu jeder Zeit den aktuellen Vorgaben entsprechen und sind nötigenfalls anzupassen.

Buchstabe a: Die Zugangs- bzw. Zugriffsrechte auf Datenbanken, welche die AHVN enthalten, dürfen nur den Mitarbeiterinnen und Mitarbeitern eingeräumt werden, die diese zur Erfüllung ihrer Aufgaben benötigen. Die Einräumung der Befugnisse hat restriktiv zu erfolgen.

Buchstabe b: Es ist eine Person zu bezeichnen, die für die systematische Verwendung der AHVN zuständig ist. Diese hat das ISDS-Konzept gemäss Buchstabe d auf

nachweisbare Art zur Kenntnis zu nehmen. Diese Person muss auch die Kompetenz haben, Massnahmen, die gemäss ISDS-Konzept nötig sind, durchzusetzen.

Buchstabe c: Die AHVN darf nicht für andere Zwecke als für die vorgesehene Aufgabenerfüllung verwendet oder in unzulässiger Weise an Dritte weitergegeben werden. Mit der nötigen Aus- und Weiterbildung müssen die zugangs- und zugriffsberechtigten Personen informiert werden, dass sie die AHVN nur aufgabenbezogen verwenden und die Nummer an Dritte nur bekannt geben dürfen, wenn dies rechtens ist.

Buchstabe d: Die zur systematischen Verwendung der AHVN berechtigten Behörden, Organisationen und Personen sorgen dafür, dass die Betreiber ihrer Informatikmittel und Datenspeicher ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellen, das die einzelnen Sicherheits- und Datenschutzmassnahmen beschreibt. Das ISDS-Konzept benennt und bewertet die relevanten Risikofaktoren nach den Kriterien der Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit. Es spezifiziert, mit welchen konkreten Massnahmen die Informationssicherheits- und Datenschutzanforderungen umzusetzen sind. Die Implementierungsmassnahmen beziehen sich auf die Infrastruktur, die Organisation, die Schulung des Personals sowie die Anpassung von Hard- und Software.

Zum einen muss der Zugang zu Informatikmitteln und Datenspeichern physisch gesichert sein. Beim Einsatz mobiler Informatikmittel und Datenspeicher muss mit Hilfe kryptografischen Verfahren, die dem Stand der Technik entsprechen (Datenverschlüsselung), sichergestellt sein, dass der Zugriff für Unberechtigte nicht möglich ist.

Zum andern muss der Zugriff auf Informatikmittel und Datenspeicher mit Hilfe von zusätzlichen – dem Stand der Technik entsprechenden und der Risikolage angepassten – Informatiksicherheitsmassnahmen geschützt sein. Diese Massnahmen müssen mindestens den Einsatz von handelsüblicher, aktueller Software zur Entdeckung und Beseitigung von Malware (Antiviren-Software) sowie den Einsatz von (zentralen oder persönlichen) Firewall-Systemen umfassen. Wer auf Informatikmittel und Datenspeicher zugreifen kann, muss sich vorher authentifizieren müssen. Wird für die Authentifizierung ein Passwort eingesetzt, ist dieses geheimzuhalten. Es darf nicht weitergegeben werden, und es ist unverzüglich zu ändern, wenn Verdacht besteht, dass Unberechtigte davon Kenntnis haben. Ferner ist die Betriebs- und Anwendungssoftware von Informatikmitteln möglichst zeitnah mit aktuellen Fehlerbehebungs-Updates (Patches) auszurüsten. Wichtige Aktivitäten und Ereignisse auf Informatiksystemen sind aufzuzeichnen und regelmässig auszuwerten. Vor der Reparatur, Entsorgung oder Vernichtung von Informatikmitteln und Datenspeichern muss ausserdem sichergestellt sein, dass sie weder AHVN noch andere Personendaten mehr enthalten und dass solche nicht rekonstruiert werden können.

Schliesslich besteht beim Datentransfer über öffentliche Netze das Risiko, dass Daten in den Besitz von Personen gelangen können, für welche sie nicht bestimmt sind. Als öffentlich zu betrachten ist jedes Netz, das nicht einem abschliessend definierten und besonderen Zutrittskontrollen unterworfenen Kreis von Nutzerinnen und Nutzern vorbehalten ist (z. B. amtsinternes Netz). Mit einer dem aktuellen Stand der Technik entsprechenden Verschlüsselung kann dieser Gefahr begegnet werden.

Buchstabe e: Im Rahmen eines Notfallkonzepts muss bestimmt werden, wie im Falle eines missbräuchlichen Zugriffs auf Datenbanken oder einer missbräuchlichen Nutzung derselben vorzugehen ist. Diese Regelung der gegebenenfalls erforderlichen Massnahmen bildet ebenfalls Teil des ISDS-Konzepts.

Art. 153e Risikoanalyse

Absatz 1: Periodische Risikoanalysen sollen dazu dienen, unerlaubte Zusammenführungen von Datenbanken zu erkennen und nötigenfalls die Verwaltungen dazu zu veranlassen, so zusammenzuarbeiten, dass die technischen und organisatorischen Massnahmen gestützt auf eine realistische und aussagekräftige Einschätzung der systemischen Gesamtrisiken getroffen werden.

Die *Buchstaben a* und *b* legen fest, welche Einheiten auf der Ebene des Bundes und der Kantone die Risikoanalyse durchführen müssen und für welche Datenbanken.

Absatz 2: Die Verzeichnisse von Datenbanken, welche die AHVN enthalten, ermöglichen ein gezieltes und koordiniertes Vorgehen bei der Risikoanalyse. Dieses Ziel kann auch dadurch unterstützt werden, indem bereits existierende Verzeichnisse von Datenbanken nach dem Kriterium der systematischen Verwendung der AHVN erschlossen werden.

Art. 153f Mitwirkungspflichten

Wer die AHVN systematisch verwendet, hat ferner verschiedene Mitwirkungspflichten gegenüber der ZAS. Diese dienen in erster Linie der Zuverlässigkeit der AHVN.

Buchstabe a: Die ZAS ist darauf angewiesen, von den Berechtigten orientiert zu werden, wenn sie von ihrer Berechtigung zur systematischen Verwendung der AHVN Gebrauch machen. Darum stehen diejenigen, die die AHVN ausserhalb der AHV verwenden, auch nach dem revidierten Recht gegenüber der ZAS in der Pflicht, dies zu melden. Diese Meldepflicht soll auf der Gesetzesstufe verankert werden. Künftig wird die ZAS zu prüfen haben, ob es sich bei Einheit, die die systematische Verwendung der AHVN meldet, um eine Behörde handelt bzw. ob eine spezialgesetzliche Grundlage für Private gemäss Artikel 153*c* Absatz 1 Ziffer 4 mit Verwaltungsaufgabe besteht.

Buchstaben b und c: Durch diese Mitwirkungspflichten soll sichergestellt werden, dass die ZAS Datenabgleiche für die Verifizierung der verwendeten Nummern veranlassen oder durchführen kann und die von ihr nötigenfalls angeordneten Korrekturen vorgenommen werden.

Art. 153g Bekanntgabe der AHVN beim Vollzug von kantonalem oder kommunalem Recht

Diese Bestimmung entspricht inhaltlich weitgehend dem geltenden Artikel 50*f*. Die Änderung gegenüber dem bisherigen Recht besteht darin, dass sie auch erfasst, wer kommunales Recht vollzieht und die AHVN systematisch verwendet. Dies, weil die AHVN neu auch zum Vollzug von kommunalem Recht verwendet werden darf. Im Interesse des Datenschutzes wird festgelegt, unter welchen Voraussetzungen diese

Verwender die AHVN im Einzelfall Dritten bekanntgeben dürfen. Dabei sind die im entsprechenden Aufgabengebiet jeweils geltenden rechtlichen Vorgaben für die Datenbekanntgabe zu beachten.

Die Bekanntgabe der AHVN durch Bundesorgane richtet sich weiterhin nach den – inhaltlich gleich ausgestalteten – Bestimmungen des DSG.

Art. 153h Gebühren

Bereits nach geltendem Recht können gestützt auf Artikel 46*a* RVOG Gebühren erhoben werden für den Aufwand, welcher der ZAS im Zusammenhang mit der systematischen Verwendung der AHVN ausserhalb der AHV entsteht. Da die systematische Verwendung der AHVN ausserhalb der AHV erweitert wird, soll zur Verbesserung der Transparenz die Möglichkeit der Gebührenerhebung im AHVG verankert werden (vgl. Ziff. 6.1).

Art. 153i Strafbestimmungen des vierten Teils

Absatz 1: Die neue Regelung deckt sich materiell mit jener gemäss dem geltenden Artikel 87 achtes Lemma. Wie bisher untersteht die unbefugte systematische Verwendung der AHVN einer Geldstrafe.

Absatz 2: Bei dieser Bestimmung handelt es sich um eine Weiterführung der bisherigen Regelung gemäss Artikel 88 viertes Lemma. Die Übertretung ist sowohl bei vorsätzlicher als auch bei fahrlässiger Begehung strafbar (Art. 333 Abs. 7 des schweizerischen Strafgesetzbuchs[39]).

Absatz 3: Da das ATSG auf den 4. Teil nicht anwendbar ist, ist ein Verweis auf Artikel 79 ATSG erforderlich, damit die oben erwähnten Strafbestimmungen auch auf die Widerhandlungen in Geschäftsbetrieben Anwendung finden.

Gliederungstitel vor Art. 154

Fünfter Teil: Schlussbestimmungen

Die systematische Verwendung der AHVN ausserhalb der AHV ist neu im vierten Teil des Gesetzes geregelt. Dadurch sind die Schlussbestimmungen in einem fünften Teil enthalten.

Schlussbestimmungen

Damit die Stellen und Institutionen, welche die AHVN bereits systematisch verwenden, die nötigen Umstellungen realisieren können, ist ihnen eine Übergangsfrist einzuräumen. Da sie nach geltendem Recht schon technische und organisatorische Massnahmen treffen mussten, ist die Frist von einem Jahr angemessen.

39 SR **311.0**

Änderung anderer Erlasse

In anderen Erlassen sind die Bestimmungen zur systematischen Verwendung der AHVN ausserhalb der AHV zu ändern beziehungsweise zu streichen. Doppelspurigkeiten gilt es zu vermieden. Ausserdem sollen die verschiedenen verwendeten Begriffe durch «AHV-Nummer» ersetzt werden.

5.2 Koordinationsbedarf mit anderen Revisionsvorlagen

Aufgrund des laufenden Revisionsprojekts «Modernisierung der Aufsicht in der 1. Säule und Optimierung in der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge» besteht Koordinationsbedarf. Unabhängig davon, ob das Revisionsprojekt «Modernisierung der Aufsicht in der 1. Säule und Optimierung in der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge» oder der vorliegende Gesetzesentwurf zuerst in Kraft tritt, werden die Änderungen des Ersteren massgebend sein, mit Ausnahme des Begriffs «Versichertennummer», der im ganzen Erlass durch «AHV-Nummer» ersetzt werden soll.

6 Auswirkungen

6.1 Finanzielle und personelle Auswirkungen auf den Bund

Durch die Möglichkeit der erweiterten Verwendung der AHVN werden bei der ZAS zunächst mehr neue Meldungen zum Zugang zu den angebotenen Diensten eingehen. Es ist mit zusätzlichen Anfragen von Nutzerinnen und Nutzern zu rechnen. Dies verursacht im laufenden Betrieb höhere Kosten. Wie hoch sie sein werden, ist schwer zu prognostizieren. Sie hängen stark davon ab, wie viele Einheiten die AHVN neu systematisch verwenden möchten und wie sie sich in Bezug auf die Nutzung verhalten. In einer Übergangszeit von zwei bis fünf Jahren wird mit einem Anstieg der Nutzermeldungen und der Anträge für den Zugang zu den ZAS-Diensten gerechnet. Der Zusatzaufwand wird mit den bestehenden personellen Ressourcen bewältigt.

Höhere Ausgaben werden auch für die Infrastruktur der UPI-Datenbank entstehen, da eine steigende Nutzerzahl einen Einfluss auf die Kapazität der Informatiksysteme hat. Was die Modernisierung der Anwendungen zur Verwaltung der Meldungen für die systematische Verwendung der AHVN und des Zugangs zu den Diensten der ZAS angeht, ist mit Investitionskosten zwischen 500 000 Franken und einer Million Franken zu rechnen. Die Kosten für eine stärkere automatische Aufsicht über die Nutzung der ZAS-Dienste dürften mit 200 000 bis 750 000 Franken zu Buche schlagen. Die gesamthaften Zusatzkosten für die Investitionen bewegen sich somit zwischen 700 000 Franken und 1,75 Millionen Franken.

Nach geltendem Recht hat der Bundesrat die Möglichkeit, Gebühren zu erheben für die Zusatzkosten im Zusammenhang mit der Verwendung der AHVN ausserhalb der AHV. Die Gebührenpflicht ist in den Artikeln 134^{sexies} und 134^{septies} AHVV konkre-

tisiert. Da zahlreiche Ausnahmen vorgesehen sind, werden in der Praxis kaum Gebühren erhoben. Die Kosten, die nicht durch Gebühren finanziert sind, werden von der ZAS bzw. die Ausgleichsfonds getragen. Letztere werden hauptsächlich durch Beiträge der Versicherten und der Arbeitgeber, durch den Beitrag des Bundes und der Mehrwertsteuer finanziert. Erbringt die ZAS Dienstleistungen für Fremdnutzer der AHVN, soll dies aber die Sozialversicherungen der 1. Säule nicht belasten. Da die systematische Verwendung der AHVN ausserhalb der AHV erweitert wird, soll zur Verbesserung der Transparenz die Möglichkeit der Gebührenerhebung im AHVG verankert werden. Eine Überarbeitung der aktuell gültigen Ausnahmeregelung muss auf Verordnungsebene erfolgen. Dadurch können die Kosten für die erweiterte Verwendung auf die betreffenden Verwender, also die Kostenverursacher, überwälzt werden.

Als kostenreduzierender Faktor treten schliesslich Effizienzgewinne bei den Bundesbehörden, die neu die AHVN nutzen werden, ein. Die verbesserte Qualität des Datenbestands bei den Behörden erleichtert und beschleunigt die Verwaltungstätigkeit. Sie ermöglicht auch einen unkomplizierten, d. h. möglichst automatischen Datenfluss, zwischen den Behörden. Die generelle Berechtigung von Behörden hat ausserdem zur Folge, dass nicht mehr für jeden neuen Verwendungszweck spezifisch eine gesetzliche Grundlage geschaffen werden muss. Dadurch werden auch die gesetzgebenden Behörden entlastet. Allerdings müssten gegebenenfalls die Begleitmassnahmen aktualisiert werden, wodurch zusätzliche Kosten entstehen können. Die Höhe der zusätzlichen Einsparungen und Ausgaben lässt sich nicht beziffern.

6.2 Finanzielle und personelle Auswirkungen auf Kantone und Gemeinden

Werden für die systematische Nutzung der AHVN Gebühren erhoben, so entstehen bei den Kantonen und Gemeinden zusätzliche Kosten. Diese können erst nach Kenntnis des Gebührensystems und der Ausnahmeregelungen geschätzt werden, sie dürften allerdings gering sein. Zudem verursacht die Meldepflicht bei den Nutzerinnen und Nutzern einen (vernachlässigbaren) Initialaufwand.

Zugleich sind die Effizienzgewinne bei der Verwaltungstätigkeit (siehe Ziff. 6.1) bei Kantonen und Gemeinden ein kostenreduzierender Faktor. Es ist davon auszugehen, dass die einzelnen Behörden die allfälligen Kosten gegenüber dem Nutzen für ihre Verwaltungstätigkeit abzuwägen vermögen und daher die AHVN nur nutzen werden, wenn es sich für sie wirtschaftlich lohnt. Bei Kantonen und Gemeinden ist somit von einer positiven Auswirkung auszugehen. Auch der Aufwand der gesetzgebenden Behörden von Kantonen und Gemeinden wird vermindert, weil nicht mehr für jeden neuen Verwendungszweck spezifisch eine gesetzliche Grundlage geschaffen werden muss. Wie bei den Behörden des Bundes sind allerdings die Begleitmassnahmen anzupassen, wodurch Mehrkosten entstehen, die sich nicht beziffern lassen.

6.3 Auswirkungen auf die Volkswirtschaft

Es gibt keine direkten volkswirtschaftlichen Auswirkungen aus der Vorlage. Indirekte positive Auswirkungen entstehen hingegen infolge der Verbesserung des elektronischen Verkehrs zwischen Bürgerinnen und Bürgern und Behörden sowie zwischen den Behörden, sie sind allerdings nicht quantifizierbar.

6.4 Auswirkungen auf die Gesellschaft

Die Vorlage hat keine direkten Auswirkungen auf die Gesellschaft.

6.5 Auswirkungen auf die Umwelt

Die Vorlage hat keine direkten Auswirkungen auf die Umwelt.

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

7.1.1 Kompetenzen

Die Vorlage stützt sich auf die Kompetenznormen der Bundesverfassung, die den Bund zur Rechtsetzung im Bereich der Alters- und Hinterlassenenversicherung ermächtigen (Art. 111 und 112 BV). Soweit die Regelungen zur AHVN deren Verwendung als generellen Personenidentifikator für Behörden betreffen, ergibt sich die Kompetenz des Bundes aus Artikel 173 Absatz 2 BV, der dem Bund die Kompetenz zur Regelung der Organisation der Bundesbehörden überträgt. Ermöglicht der Bundesgesetzgeber den Kantonen und – vorbehältlich anderslautenden kantonalen Rechts – den Gemeinden, die AHVN systematisch zu verwenden, ist er zugleich befugt, die Voraussetzungen der Nutzung dieses Instruments zu definieren und entsprechende Vorschriften zu erlassen.

7.1.2 Persönlichkeitsschutz

Die Vorlage ist auch unter dem Aspekt von Artikel 13 Absatz 2 BV verfassungskonform. Die vorgeschlagenen Änderungen des AHVG regeln hinlänglich, unter welchen Voraussetzungen die systematische Verwendung der AHVN erlaubt sein soll. Das Erfordernis der hinreichenden gesetzlichen Grundlage ist daher erfüllt. Der Grundsatz der Zweckbindung ist ebenfalls eingehalten, indem die Nutzerinnen und Nutzer die AHVN ausschliesslich zur Erfüllung ihrer gesetzlichen Aufgaben systematisch verwenden dürfen. Zudem enthält der Vorentwurf Leitplanken zu den einzuhaltenden sichernden Massnahmen sowie Regelungen zu den Konsequenzen von Verletzungen dieser Vorgaben (vgl. Ziff. 4.2).

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Vom Themenbereich der Vorlage sind keine internationalen sozialrechtlichen Verpflichtungen der Schweiz betroffen.

7.3 Erlassform

Nach Artikel 164 Absatz 1 BV sind alle wichtigen rechtsetzenden Bestimmungen in der Form eines Bundesgesetzes zu erlassen. Dies ist mit dieser Vorlage gewährleistet.

7.4 Unterstellung unter die Ausgabenbremse

Die Vorlage untersteht nicht der Ausgabenbremse nach Artikel 159 Absatz 3 Buchstabe b BV, da sie weder Subventionsbestimmungen noch die Grundlage für die Schaffung eines Verpflichtungskredites oder Zahlungsrahmens enthält.

7.5 Delegation von Rechtsetzungsbefugnissen

Artikel 153*h* delegiert dem Bundesrat die Möglichkeit, Gebühren vorzusehen für die Dienstleistungen, welche die Zentrale Ausgleichsstelle im Zusammenhang mit der systematischen Verwendung der AHVN ausserhalb der AHV erbringt.