Kompetenzzentrum Öffentliche IT

Fraunhofer FOKUS

Technische Perspektiven der Registermodernisierung

Peter Parycek, Simon Sebastian Hunt & Basanta E.P. Thapa

Stand: 8. Februar 2021

Einleitung

Nur mit datenschutzkonformen und harmonisierten Verwaltungsregistern können Onlinezugangsgesetz (OZG), die EU-Verordnung zum Single Digital Gateway (SDG-VO) und der Registerzensus umgesetzt werden. Das Registermodernisierungsgesetz (RegMoG) ist die rechtliche Grundlage für eine Harmonisierung und Vernetzung der diversifizierten deutschen Registerlandschaft unter Wahrung der Datenschutzrechte und einer Stärkung der Datenschutzgrundsätze nach Art. 5 DSGVO. Im Zentrum der Debatte zum Entwurf des Registermodernisierungsgesetzes steht die Einführung einer Identifikationsnummer in Form der Steueridentifikationsnummer. Die Kritik verweist meist auf das Volkszählungsurteil[1], welches in einem Personenkennzeichen die Grundlage für eine umfassende Profilbildung gesehen hat.[2]

Um die Bildung eines digitalen Persönlichkeitsprofils zu verhindern, ist die Sicherung der Datenabfragen aus den Registern entscheidend, nicht das Verbot einer Identifikationsnummer.

Im datenreichen 21. Jahrhundert ist fraglich, inwieweit eine einheitliche Identifikationsnummer weiterhin eine notwendige technische Voraussetzung zur Erstellung digitaler Persönlichkeitsprofile ist. Die Menge an Datenpunkten in den verschiedenen staatlichen Registern reicht aus, um auch ohne Identifikationsnummer Datensätze von Bürgerinnen und Bürgern mit hoher Trefferwahrscheinlichkeit zuordnen zu können. Daher sind die Sicherungsmaßnahmen für den Zugang zu Daten entscheidend, die im RegMoG-E vorgesehen sind:

- Minimierung der Zugriffsmöglichkeiten durch örtlich verteilte Register,
- revisionssichere Protokollierung aller Datenabrufe,

[1] BVerfGE 15.12.1983, 1 BvR 209/83.
[2] BVerfGE 15.12.1983, 1 BvR 209/83, Rn 169.

- Ex-ante-Prüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen mit dem 4-Corner-Modell
- Ex-post-Prüfung durch die Bürgerin und den Bürger mithilfe eines Datencockpits.

Nur vermeintlich höherer Datenschutz durch bereichsspezifische Kennzeichen.

Das sogenannte "österreichische Modell" soll mit bereichsspezifischen Personenkennzeichen einer umfassenden Profilbildung vorbeugen. Aus technischer Perspektive ist vor allem der Zugriff auf die Register für eine Profilbildung entscheidend. Denn auch ohne eindeutige Kennzeichen können Datensätze mithilfe übereinstimmender Merkmale zu einem umfassenden Profil zusammengeführt werden.

Bereichsspezifische Kennzeichen schaffen keinen bzw. geringen zusätzlichen Schutz vor Profilbildung, führen aber zu einem wesentlichen Datenschutzproblem und zwei Datensicherheitsproblemen.

- Die notwendige Kommunikation zwischen den Tabellen oder Algorithmen zur Übersetzung der Kennzeichen zwischen den Bereichen erhöht den Datenverkehr und führt zu mehrfacher Speicherung von personenbezogenen Daten. Dies steht im Widerspruch zum Prinzip der Datenminimierung.
- Das Speichern bereichsspezifischer Personenkennzeichen erhöht die Anzahl der Komponenten im Gesamtsystem. Dies eröffnet insgesamt mehr Angriffsvektoren, denn personenbezogene Daten müssen entweder an mehreren Stellen gespeichert werden oder über einen Flaschenhals übertragen werden; wodurch das Risiko an einer Stelle gebündelt und fokussiert wird.
- In der Theorie sind die Modelle beliebig kombinierbar. In der Praxis sind Kombinationslösungen mit einem hohen Risiko des Scheiterns verbunden und führen damit zu hohen Sicherheitsrisiken und dem politischen Risiko, eine Architektur zu beschließen, die kaum erfolgreich und zeitnah implementierbar ist.

Die genauen Hintergründe dieser Beurteilung sollen im Folgenden anhand technischer Erwägungen aufgezeigt werden.

Kernprinzipien von 4-Corner-Modell und der Identifikationsnummer

Das 4-Corner-Modell ist eine IT-Architektur nach dem Prinzip des „Privacy by Design". Kern ist die dezentrale Datenhaltung in getrennten Registern bei gleichzeitiger eindeutiger Zuordenbarkeit über eine zentrale Personenidentifikationsnummer und die kontrollierte Kommunikation über Intermediäre.

Trennung von Datenbeständen (*Separate*-Prinzip)

Personenbezogene Daten liegen überwiegend in fachlich und föderal getrennten Registern, die jeweils zugriffsgeschützt sind. Die physische Trennung der Daten nach fachlichen, geografischen und/oder Ebenen-Gesichtspunkten ist eine der effektivsten Schutzformen gegen Datenmissbrauch, weil selbst im Fall eines technischen oder menschlichen Fehlers nur lokale Daten korrumpiert werden können.

Verwendung eines Pseudonyms (Prinzip der Datenminimierung)

Als zufällige Ziffernfolge bildet die Identifikationsnummer unmittelbar keine weiteren personenbezogenen Attribute über eine Person ab. Sie ersetzt in der Kommunikation zwischen den Registern personenbezogene Daten wie Namen und Geburtsdaten, die zuvor zur Zuordnung der Datensätze mitübertragen werden mussten. Da die Identifikationsnummer die eindeutige Zuordenbarkeit der Datensätze über die Register hinweg garantiert, kann die Mehrfachhaltung von personenbezogenen Daten („Datenkranz") in den Registern verringert werden und im Idealfall zukünftig auch entfallen.

Verteilte Zugangselemente

Für das Abfragen eines Datensatzes in einem anderen Register werden mehrere Faktoren benötigt: 1) Personenidentifikationsnummer, 2) digitale Adresse des Registers und des vorgeschalteten IT-Dienstleisters, 3) ein gültiges Sicherheits-Token, das die Zugangsberechtigung zum Register bezeugt. Die drei Elemente sind auf verschiedene Stellen verteilt und müssen für den Datenaustausch zusammenarbeiten, dies erhöht den Aufwand für einen missbräuchlichen Zugang erheblich.

Rechteprüfung und Verschlüsselung der Datenübertragung

Registerdaten werden nur bei bestandener Prüfung der Zugangsberechtigung übertragen. Die Datenübertragung erfolgt verschlüsselt, sodass nur Absender und Empfänger, aber keine zwischengeschalteten Stellen die Inhalte einsehen können.

Punktgenaue Datenabfrage

Anfragende Behörden erhalten nur die Inhaltswerte der von ihnen erbetenen Datenfelder und nur bzgl. der genannten Personenidentifikationsnummer zugesandt. Sie haben weder selbsttätigen Zugriff auf Register noch können sie diese beliebig durchsuchen.

Transparenz und Kontrolle der Datenverarbeitung

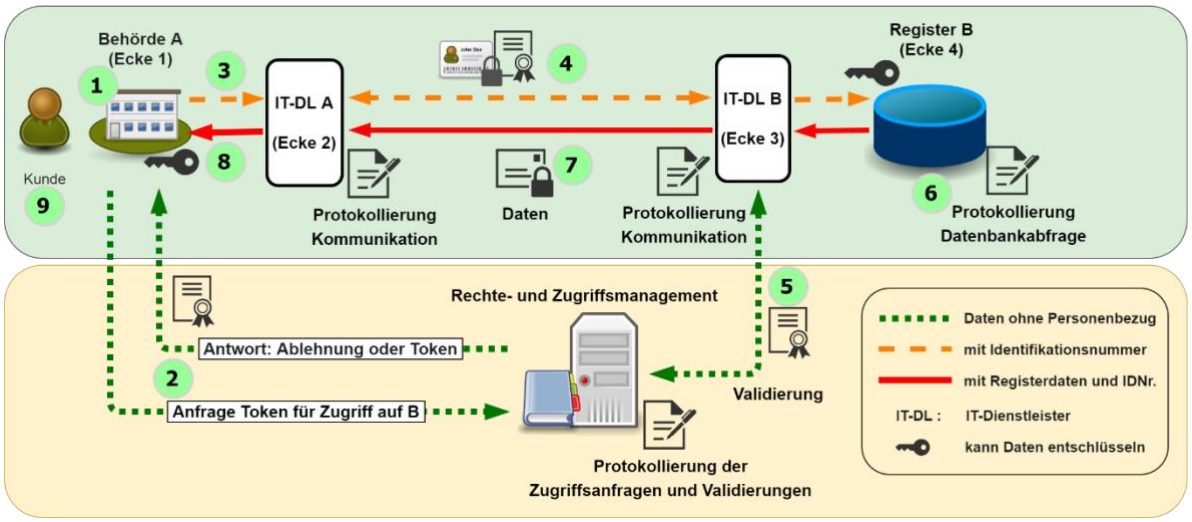
Datenübertragungen und Anfragen in der Registerlandschaft werden – ohne Inhaltswerte – von jeder beteiligten Stelle protokolliert. Mithilfe der Identifikationsnummer können Datenbestände und Vorgänge eindeutig einer Person zugeordnet und so im persönlichen Datencockpit nachvollzogen werden. Dies schafft Transparenz und Kontrollmöglichkeiten für Betroffene und Datenschützende.

Das 4-Corner-Modell hat sich vielfach bewährt und ist neben einigen Verwaltungsbereichen auch großflächig im Bereich der Finanzverwaltung im Einsatz. Entscheidend ist für dieses System, dass das Rechte- und Zugriffsmanagement so sicher wie möglich umgesetzt wird. Denkbar sind hierfür diverse Herangehensweisen. Wie auch bei anderen komplexen Systemen ist ebenso sicherzustellen, dass keine Single Points of Failure (SPoF) oder Flaschenhälse entstehen, und keine umfassenden Datenbestände durch zentral Angriffe gewonnen werden können.

Das 4-Corner-Modell wird nur für bereichsübergreifende Kommunikation verpflichtend vorgeschrieben. Dies ermöglicht einerseits den jeweiligen Bereichen weiter eine gewisse Flexibilität in der Gestaltung ihrer IT-Strukturen und folgt der Annahme, dass die Bereiche so gewählt werden, dass die Datenbestände nicht ausreichen, um umfassende Profile zu bilden. Hinzu kommt, dass die Bereiche nur die fachspezifisch benötigten Daten speichern und so grundsätzlich eine Nähe zu den

Daten vorliegt. Dies bedeutet im Umkehrschluss jedoch nicht, dass innerhalb der Bereiche ein uneingeschränkter Zugriff auf die Daten möglich ist. Auch hier sind bereits Prozesse etabliert, die sicherstellen, dass die Berechtigung zur Verarbeitung der entsprechenden Daten besteht. Auch innerhalb der Bereiche bietet die eindeutige Identifikationsnummer die Grundlage für die Transparenz und Kontrolle der Datenverarbeitung. Zukünftig ist auch davon auszugehen, dass das 4-Corner-Modell innerhalb der Bereiche für sensible Transaktionen zum Einsatz kommt. Diese Entwicklungen sind zu beobachten und wie vorgesehen auch regelmäßig zu evaluieren.

Das 4-Corner Modell



Das abgebildete Modell zeigt eine mögliche Umsetzung bereichsübergreifender Registerabfragen im 4-Corner-Modell mit einer eindeutigen Personenidentifikationsnummer. Behörde A (Ecke 1) und Register B (Ecke 4) befinden sich entsprechend in unterschiedlichen Bereichen. Die grün umrandeten Zahlen nummerieren die Prozessschritte, die weitgehend automatisiert stattfinden:

(1) Behörde A (Ecke 1) benötigt aufgrund eines Vorgangs Daten aus Register B.

(2) Die Behörde fragt nun beim Rechte- und Zugriffsmanagement an, ob sie auf Daten des Registers B zugreifen darf. Das Zugriffsmanagement ermittelt anhand vorgegebener Parameter, ob eine Zugriffsberechtigung besteht. Bei einem positiven Prüfungsergebnis sendet das Zugriffsmanagement einen Sicherheits-Token an Behörde A. Dieser Token gleicht einer Zugangskarte, die bei Verwendung entwertet wird oder nach Ablauf einer vorgegebenen Zeit automatisch ihre Gültigkeit verliert. Das Zugriffsmanagement protokolliert die Anfrage und ihr Prüfungsergebnis.

(3) Behörde A füllt die Elemente ihrer Datenanfrage nun in einen digitalen, mehrschichtigen Briefumschlag: Die Personenidentifikationsnummer, eventuell notwendige Basisdaten zur Person und die angefragten Datenfelder. Behörde A verschlüsselt den digitalen Briefumschlag, der erst am Register B wieder entschlüsselt (= geöffnet) werden kann. Den digitalen Briefumschlag sendet Behörde A nun zusammen mit dem in Schritt 2 erhaltenen Sicherheits-Token an ihren IT-Dienstleister A. Dieser IT-Dienstleister übernimmt die Funktion des Intermediärs (Ecke 2). Behörde A protokolliert den gesamten Vorgang bei sich.

(4) IT-Dienstleister A ermittelt über ein zentrales Verzeichnis die digitale Adresse des für Register B zuständigen IT-Dienstleisters B (Ecke 3). Auf dieses Adressverzeichnis hat die Behörde A keinen Zugriff. IT-Dienstleister A sendet die verschlüsselte Anfrage von Behörde A mit dem zugehörigen Sicherheits-Token an IT-Dienstleister B. Die IT-Dienstleister protokollieren die erfolgte Kommunikation.

(5) IT-Dienstleister B erhält die Anfrage und prüft durch das Validieren des erhaltenen Sicherheits-Tokens beim Zugriffsmanagement, ob er die Anfrage an Register B weitergeben darf. Ist das Token gültig, gibt IT-Dienstleister B die Anfrage an Register B weiter. Das Zugriffsmanagement protokolliert die Prüfung und markiert den Token bei sich als entwertet. Kann das Zugriffsmanagement die Gültigkeit des Sicherheits-Tokens nicht bestätigen, meldet IT-Dienstleister B dies an den IT-Dienstleister A zurück, der wiederum Behörde A informiert. IT-Dienstleister B protokolliert die Vorgänge.

(6) Behörde B erhält die Anfrage und entschlüsselt sie. Mithilfe der Personenidentifikationsnummer ermittelt sie in Register B den korrekten Datensatz. Die Inhaltswerte der angefragten Datenfelder kommen zusammen mit der Personenidentifikationsnummer in einen digitalen Briefumschlag, den Behörde B verschlüsselt. Behörde B sendet diesen auf bekanntem Wege via IT-Dienstleister B und A an Behörde A. Behörde B protokolliert den Vorgang ohne die angefragten Inhaltswerte.

(7) IT-Dienstleister B ermittelt über das Verzeichnis die digitale Adresse des IT-Dienstleisters A und gibt die verschlüsselten Daten weiter.

(8) Die Behörde A empfängt und entschlüsselt das Paket von IT-Dienstleister A. Behörde A ordnet die übermittelten Inhaltswerte durch die Personenidentifikationsnummer eindeutig zu und verwendet sie für den benötigten Zweck. Behörde A löscht die Inhaltswerte, sobald ihr Zweck, etwa die Prüfung einer Anspruchsvoraussetzung, erfüllt ist. Behörde A protokolliert diese Vorgänge.

(9) Die für die Nachvollziehbarkeit der Datenverarbeitung benötigten Protokolldaten werden dem Betroffenen in seinem Datencockpit angezeigt, sobald er diese abruft.

Technische Schutzaspekte

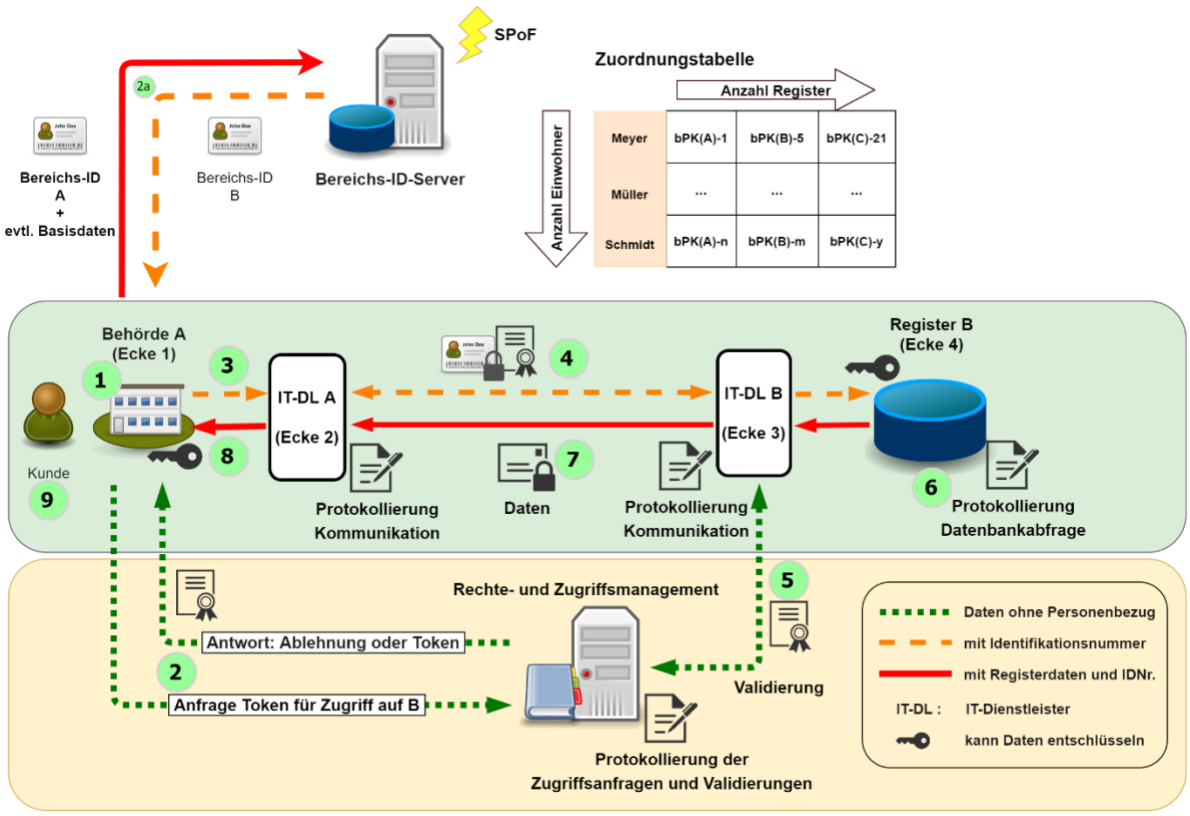
Die eindeutige Personenidentifikationsnummer ermöglicht in diesem System, dass Behörde A und Register B wissen, über welche Person sie sprechen. Aufgrund der Eindeutigkeit kann im Idealfall auf die Übermittlung von weiteren personenbezogenen Daten in Form eines Datenkranzes verzichtet werden bzw. wird die Anzahl der zusätzlich benötigten personenbezogenen Daten stark reduziert werden können. Aktuell werden zwischen Behörden Datenkränze bzw. sogenannte Basisdaten ausgetauscht, die Daten beinhalten, die nicht relevant für das Verfahren sind, aber für die eindeutige Identifikation von Personen benötigt werden. Diese aktuelle Verwaltungspraxis steht im Widerspruch zu dem Datenschutzgrundsatz der Datenminimierung der DSGVO. Die ID-Nr. selbst ist kein sprechendes Datum. Sollte sie Unbefugten bekannt werden, können sie diese nicht verwerten. Sie ist im Kern ein Kommunikationswerkzeug für die Verwaltung, das sicherstellt, dass Datensätze richtig zugeordnet werden können. Alleinstehend berechtigt sie an keiner Stelle der Verarbeitungskette zum Zugriff auf Daten, ohne dass die anfragende Stelle eine zusätzliche zweifelsfreie Berechtigung

nachweisen kann. Ebenso wird die Kommunikation dieser Identifikationsnummer noch technisch über das verschlüsselte Couvert abgesichert. Wird dieses abgefangen, können Dritte nicht auf Inhalte zugreifen, die übermittelt werden.

Die wichtigste Sicherungsfunktion in diesem Modell ist jedoch das Rechte- und Zugriffsmanagement in Kombination mit dem 4-Corner-Modell. Der Begriff des Zugriffsmanagements ist in dieser Kombination etwas missverständlich. Die anfragende Behörde bekommt keinen tatsächlichen Zugriff auf das Register. Sie bekommt lediglich jene Daten ausgehändigt, die sie anfragt und für die sie eine Berechtigung hat. Andere Arten von Anfragen können technisch ausgeschlossen werden. Einerseits dadurch, dass der anfragenden Behörde nicht bekannt ist, wie sie das Register erreichen soll. Andererseits kann das Register nur auf bestimmte Anfragen reagieren. Ein systematisches Durchsuchen aller Register mit der Personenidentifikationsnummer ist so nicht möglich. In jedem Fall würde der Versuch zu einer umfassenden Datenspur in den Protokollierungen führen. Denn die die ID-Nr. ermöglicht, dass Betroffene, Datenschutzbeauftragte und Vorgesetze in der Lage sind, die Verwendung der Daten nachzuverfolgen und zweifelhafte Abfragen zu rügen bzw. der Strafverfolgung zuzuleiten. Hierfür sind in einem solchen System keine Inhaltsdaten notwendig. Im Ergebnis wird auch die Schutzwirkung des Strafrechts gegenüber internem Missbrauch gestärkt, da eine unabhängige Kenntnisnahme und Kontrolle der Datenverarbeitung durch Bürgerinnen und Bürger erstmals möglich wird.

Auf der föderalen Ebene wird dieses Sicherungssystem noch dadurch ergänzt, dass die Register weiterhin dezentral geführt werden. Der in der Grafik aufgeführte Kommunikationsprozess lässt diesen Aspekt ein Stück weit außer Acht. Behörde A und Register B sind nicht nur durch Bereiche getrennt, sondern stehen eventuell auch in verschiedenen Bundesländern. Dies ermöglicht das Sicherungssystem der vertikalen Gewaltenteilung des Föderalismus in der Arbeitsweise des Registersystems zu spiegeln. Nicht nur die Kontrolle der Datenverarbeitung über die Protokollierungen im System ist föderal verteilt, sondern auch die tatsächliche Kontrolle der Datenzentren. Im Fall einer schweren demokratischen Krise beispielsweise könnte die zentrale bundesweite Zusammenführung der Daten durch Länder und Kommunen durch eine technische Entkoppelung verhindert werden.

4-Corner-Modell mit bereichsspezifischen Kennzeichen



Die Bildung umfassender Persönlichkeitsprofile hat das Bundesverfassungsgericht im Volkszählungsurteil von 1983 untersagt und damals in einer eindeutigen Identifikationsnummer eine Voraussetzung für die Erstellung von Profilen gesehen.[3] Inwieweit diese Aussage unter heutigen Umständen noch weiter Geltung hat, ist umstritten. Diejenigen, die in der bloßen Existenz einer eindeutigen bzw. einheitlichen Identifikationsnummer eine Gefahr sehen, sprechen sich dafür aus, die einzelne Nummer durch bereichsspezifische Kennziffern zu einer Person ersetzt werden.

Die Einführung von bereichsspezifischen Kennziffern zieht Änderungen in den folgenden Prozessschritten nach sich:

(1) Um Daten aus anderen Registern abzufragen, muss sich Behörde A nun zusätzlich zu dem Zugriffsmanagement auch an den Bereichs-ID-Server wenden. 2a) Zunächst muss der Bereichs-ID-Server prüfen, ob Behörde A berechtigt ist, ID-Nr. aus Bereich B anzufragen. Hierfür werden Zertifikate, PKIs oder Behörden-IDs vorgeschlagen. Dieser Prozess kann auch wieder protokolliert werden. Liegt eine solche Berechtigung vor, sind mehrere Varianten denkbar, um die in Register B verwendete bereichsspezifische Kennziffer der betroffenen Person zu ermitteln:

a. Behörde A sendet die für ihren Bereich spezifische Personenidentifikationsnummer und den Zielbereich an den Bereichs-ID-Server. Der Bereichs-ID-Server betreibt eine Tabelle, in der die verschiedenen bereichsspezifischen Kennziffern einander zugeordnet sind.

[3] s.o. Fn. 1 u. 2.

Hieraus ermittelt der Bereichs-ID-Server die für Bereich B spezifische ID-Nr. zu der von Behörde A übermittelten Kennziffer und sendet sie an die Behörde.

a. Behörde A übermittelt neben der eigenen ID personenbezogene Basisdaten wie Name und Geburtsdaten an den Bereichs-ID-Server. Mithilfe der Basisdaten findet der Bereichs-ID-Server den Datensatz der betroffenen Person und sendet die Kennziffer für Bereich B an Behörde A.

b. Behörde A übermittelt neben der eigenen Kennziffer den Zielbereich, aus dem die Bereichs-ID benötigt wird. Die Bereichs-IDs werden aus einer geheimen Stammzahl erzeugt, die mit einem Begriff verhasht wird. Es besteht also weiterhin ein eindeutiges Personenkennzeichen, dieses wird aber nur zur Erzeugung von Bereichskennziffern verwendet und nicht zirkuliert. Über die geheime Stammzahl sind die Bereichs-ID einander zuordenbar und der Bereichs-ID-Server kann der Behörde A mit der Bereichskennziffer des Bereichs B antworten.

(2b-9) Wie im 4-Corner-Modell (s.o.). Statt der eindeutigen Personenidentifikationsnummer wird die Bereichskennziffer übermittelt. Allerdings wird der Prozess des Abrufens und Bewertens der Protokolldaten komplexer, da diese lediglich über den Bereichs-ID-Server aufgelöst werden können.

Technische Schutzaspekte

Das Hinzufügen des Prüfungsschritts über den Bereichs-ID Server führt in erste Linie zu einer gesteigerten Komplexität des Gesamtsystems und einem zentralen Schwachpunkt. Eine höhere Anzahl von technischen Komponenten müssen im System angesteuert werden und beim Aufbau und der Pflege Berücksichtigung finden. Dies erschwert den Ausschluss von Sicherheitslücken und die Instandhaltung des Systems. Gleichzeitig führt der hinzugefügte Bereichs-ID-Server zu einem Flaschenhals. Da lediglich diese Komponente zum Auflösen der Bereichs-IDs in der Lage ist, muss sie für jeden Schritt, der hierauf angewiesen ist, angesteuert werden. Neben dem Austausch von Daten ist hier das Nachvollziehbarmachen der Verarbeitungsschritte über die Protokolldaten bedeutsam. Würde der Bereichs-ID-Server nun ausfallen oder angegriffen werden, hätte das nicht nur zur Folge, dass der Datenaustausch allgemein zum Erliegen käme, bzw. wiederum umfassend personenbezogene Daten versendet werden müssten. Ebenso würde die Transparenz der Datenverarbeitung ausfallen. Steigert man die Redundanz dieses System, so würde dies wieder ein Mehr an vorzuhaltenden personenbezogenen Daten im Gesamtsystem (Datenkranz bzw. Basisdaten) bedeuten.

Die so gesteigerte Komplexität führt bei genauer Betrachtung zu keiner echten Steigerung der Sicherheit. Sind für die Ausfallsicherheit des Systems auch überall noch umfassend Basisdaten zu speichern, führt dies das Kernargument der bereichsspezifischen Kennziffer ad absurdum. Die Basisdaten würden so auch ohne eine Kennziffer das Zusammenführen der Daten ermöglichen. Wird das System ohne zusätzliche Basisdaten umgesetzt, steigt das Risiko einer falschen Zuordnung. Lässt man diesen Aspekt beiseite, bleibt zu klären, wie der Zugang zum Bereichs-ID-Server zu regeln ist und wo der Unterschied zum Rechte- und Zugangsmanagement allgemein liegt. Prüfen beide Stellen das gleiche, ist der Prüfungsschritt praktisch redundant. Nimmt man an, dass das Rechte- und

Zugangsmanagement sämtliche relevanten Punkte prüfen könnte, steht die Frage im Raum, warum man diese Schritte aufteilen sollte und subsequent einen der beiden schwächt. Grundsätzlich muss das Rechte- und Zugangsmanagement alle Schritte prüfen, die für einen rechtmäßigen Datenaustausch notwendig sind. Die zusätzlichen Schritte und die gesteigerte Komplexität müssten einen entsprechenden Mehrwert liefern, der diesen Aufwand rechtfertigt. Dieser ist nicht ersichtlich, sondern ganz im Gegenteil wird die Datensicherheit durch die Erhöhung der Angriffspunkte in der Gesamtarchitektur verringert und das Datenmissbrauchsrisiko durch den beschriebenen Flaschenhals erheblich erhöht.

Ebenso führt das System zu mehr personenbezogenen Daten im Gesamtsystem. Das Modell mit einer einheitlichen Personenidentifikationsnummer beinhaltet mit dem Zentralamt für Steuern eine Anlaufstelle zur Verifizierung, die für den laufenden Betrieb nicht benötigt wird. Sie ermöglicht, die korrekte Datenzuordnung im Gesamtsystem zu überwachen, ohne das System durch einen Flaschenhals fragil zu machen. Bei bereichsspezifischen Kennzeichen muss diese korrekte Zuordnung auch sichergestellt sein. Der Nachteil des Flaschenhalses lässt sich jedoch nicht ausräumen, ohne das System wiederum durch mehr Redundanz und somit auch einer erhöhten Speicherung von personenbezogenen Daten ad absurdum zu führen. Das Modell mit bereichsspezifischen Kennzeichen steht somit im direkten Widerspruch zum Datenschutzgrundsatz der Datenminimierung.

Umsetzungsvarianten

Eine Variante der Umsetzung ist die Führung einer Zuordnungstabelle. Hier werden für alle Bereiche oder Register einmalig Bereichskennzeichen erstellt und miteinander verknüpft, unabhängig davon, ob dort Daten liegen oder nicht. Aufgrund der aktuellen Datenqualität und der damit verbundenen Verwechslungsgefahr von Personen müssen weitere personenbezogene Basisdaten vorgehalten werden, um Personen eindeutig zu identifizieren.

Eine weitere diskutierte Variante erzeugt bereichsspezifische Kennzeichen nur für Bereiche, in denen ein Bedarf besteht. Damit im Verlauf neue bereichsspezifische Kennzeichen eingeführt werden können, müssen wiederum personenbezogene Basisdaten gespeichert werden, die den neuen Bestand mit bestehenden Kennzeichen verknüpfen. Diese würden wiederum den Zweck bereichsspezifischer Kennzeichen aushebeln, da die Datenbestände dann auch über die Basisdaten verknüpft werden könnten.

Alternativ wird die Verwendung einer geheimen Stammzahl vorgeschlagen. Diese Variante unterscheidet sich von der einheitlichen Personenidentifikationsnummer des RegModG nur durch die Einführung einer weiteren Kennzahl, die aufgebaut und gewartet werden muss und im Steuerbereich zu einer doppelten Speicherung der beiden Identifikationszahlen führen würde. Die gesteigerte Komplexität würde wiederum keinen entsprechend gesteigerten Schutz vor einer Zusammenführung von Datenbeständen nach sich ziehen, aber den Aufwand und die Komplexität in der Umsetzung erhöhen.

Als weitere Problematik kommt hinzu, dass in einem föderal verteilten Modell weiterhin die Möglichkeit bestehen muss, festzustellen, in welchem lokalen Register die Daten liegen. Zur Lösung dieser Problematik besteht noch kein eindeutiger Langzeitplan. Solange Fachverfahren noch auf das Vorliegen der Basisdaten angewiesen sind, müssen diese weiterhin lokal gespeichert werden und

können diese Zuordnung ermöglichen. Die Richtigkeit der Basisdaten wird über das Zentralamt für Steuern bzw. die Registermodernisierungsbehörde beim Bundeverwaltungsamt sichergestellt. Werden bereichsspezifische Kennziffern eingeführt, würde ihr Schutz durch die gespeicherten Basisdaten de facto überflüssig werden. Diese würden erneut als vergleichbares Ordnungsmerkmal grundsätzlich einen hohen Grad an Verknüpfbarkeit ermöglichen. Alternativ könnte in einem solchen Modell die Kennziffer um eine Zeichenfolge erweitert werden, die diese Zuordnung ermöglicht. In der Folge würde die Kennziffer aber zumindest zum Teil eine sprechende Form annehmen. Ließe man die Möglichkeit der lokalen Zuordnung weg, würde der Datenverkehr von personenbezogenen Daten im Gesamtsystem pro Abfrage drastisch steigen und somit wiederum der Datenminimierung entgegenstehen. Weitere Komplexität erzeugt dieses System bei einer Folgebetrachtung einzelner Verfahren. So wäre noch zu klären, wie diese lokale Zuordnung beispielsweise im Falle des Umzugs einer Person angepasst werden kann. Im 4-Corner-Modell kann diese Anpassung über eine Meldung an das Zentralamt für Steuern vorgenommen werden. Dieses verteilt die aktualisierten Basisdaten dann beim nächsten Datenabgleich.

Fazit

Der Grundgedanke einer Lösung mit bereichsspezifischen Kennzeichen nach dem österreichischen Vorbild mag auf den ersten Blick nachvollziehbar erscheinen. Bei einer genaueren Betrachtung sind die datenschutzrechtlichen Nachteile und die damit einhergehenden Datensicherheitsrisiken beim Einsatz der österreichischen Architektur in einer dezentral verteilten und lokal kontrollierten Datenstruktur erheblich:

- Die notwendige Kommunikation zwischen den Tabellen oder Algorithmen zur Übersetzung der Kennzeichen zwischen den Bereichen erhöht den Datenverkehr und führt zu mehrfacher Speicherung von personenbezogenen Daten. Dies steht im Widerspruch zum Prinzip der Datenminimierung.
- Das Speichern bereichsspezifischer Personenkennzeichen erhöht die Anzahl der Komponenten im Gesamtsystem. Dies eröffnet insgesamt mehr Angriffsvektoren, denn personenbezogene Daten müssen entweder an mehreren Stellen gespeichert oder über einen Flaschenhals übertragen werden, der das Risiko an einer Stelle bündelt und fokussier.
- In der Theorie sind die Modelle beliebig kombinierbar. In der Praxis sind Kombinationslösungen mit einem hohen Risiko des Scheiterns verbunden und führen damit zu hohen Sicherheitsrisiken und dem politischen Risiko, eine Architektur zu beschließen, die kaum erfolgreich und zeitnah implementierbar ist.

Unabhängig davon ist die Annahme, dass der Einsatz eines einheitlichen Identifikationskennzeichen zu einer Profilbildung führt bzw. diese wesentlich vereinfacht, fehlgeleitet. Entscheidend ist der Zugang zu den Daten. Dieser wird durch die dezentrale Speicherung der Daten bei Ländern und Kommunen in Kombination mit dem 4-Corner-Modell wesentlich erschwert. Eine zusätzliche Prüfungsstufe kann diesem Prozess keine weitere Sicherheit hinzufügen. Wer auf bestimmte Datenbestände zugreifen darf, kann auch die entsprechende Bereichskennziffer auflösen.

Die Beibehaltung eines dezentralen, auf die Länder verteilten Modells, das ohne zusätzliche Angriffspunkte und Flaschenhälse auskommt, ist nur mit einer einheitlichen

Personenidentifikationsnummer möglich. Gleichzeitig lässt sich der Anteil an personenbezogenen Inhaltsdaten, die für einen Austausch benötigt werden, drastisch reduzieren und der dezentrale Aufbau verteilt die Kontrolle und die Daten physisch im föderalen System. Zusammengefasst ergeben sich folgende Mehrwerte des 4-Corner-Modells mit einem einheitlichen Identifikationskennzeichen:

- Minimierung der Zugriffsmöglichkeiten durch örtlich verteilte Register,
- revisionssichere Protokollierung aller Datenabrufe,
- Ex-ante-Prüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen mit dem 4-Corner-Modell
- Ex-post-Prüfung durch die Bürgerin und den Bürger mit Hilfe des Datencockpits

Neben den datenschutzrechtlichen Vorteilen sind die Kernelemente des 4-Corner-Modelles durch das ETSI standardisiert und die Elemente teilweise im täglichen Einsatz. Somit kann in der Umsetzung auf Erfahrungswerte aufgebaut werden, wodurch die Wahrscheinlichkeit einer erfolgreichen Umsetzung steigt.

Ein flächendeckender Einsatz für alle Transaktionen bzw auch für Transaktionen innerhalb der Bereiche ist nicht empfehlenswert bzw. auch nicht realistisch, weil in den Verwaltungsbereichen bereits Anwendungen und Vernetzungen zum Austausch von Daten entwickelt wurden. Diese Umsetzungen verfügen über datenschutzrechtliche Grundlagen und Vorgaben, Maßnahmen zur Datensicherheit, Protokollierung oder auch zusätzliche Bestimmungen im Disziplinar- und Strafrecht. Die IT-Architekturen der bestehenden etablierten Datenaustauschsysteme innerhalb des jeweiligen Bereichs müssten nun nachträglich umfassenden verändert werden; neben dem notwendigen erheblichen Ressourceneinsatz besteht so auch ein erhebliches Datensicherheitsrisiko. Der Fokus in der Umsetzung sollte daher in der ersten Phase der zwingende Einsatz des 4-Corner-Modells für die bereichsübergreifende Transaktion sein und der etwaigen Prüfung für zukünftige Projekte innerhalb eines Bereichs, bspw. im Fall von besonders sensiblen Datenübertragungen. Die Protokollierung der Verarbeitung sowie der Zugang zu den Protokollierungsdaten über das Datencockpit sollte für alle Anwendungen realisiert werden, um der Bürgerin und dem Bürger einen umfassenden Einblick in die Nutzung der Daten durch den öffentlichen Sektor zu gewährleisten.