Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 D

Kompetenzzentrum Öffentliche IT

An:
Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin
an: innenausschuss@bundestag.de

Kompetenzzentrum Öffentliche IT
Kaiserin-Augusta-Allee 31
10589 Berlin
E-Mail: info@oeffentliche-it.de
Telefon: +49 (0) 30 3463-7173
Fax: +49 (0) 30 3463-997173

Analyse der rechtlich-technischen Gesamtarchitektur des Entwurfs des Registermodernisierungsgesetzes

von Peter Parycek[1,2], Verena Huber[2], Simon S. Hunt[1], Anna-Sophie Novak[2] & Basanta E.P. Thapa[1]

Fraunhofer FOKUS

[1] Kompetenzzentrum Öffentliche IT (ÖFIT) am Fraunhofer-Institut FOKUS
[2] Department für Electronic Governance an der Donau-Universität Krems

Inhaltsverzeichnis

THESEN 3

I. NUTZEN EINER HARMONISIERTEN REGISTERLANDSCHAFT 7

II. DATENNUTZUNGSPRAXIS IM ÖFFENTLICHEN SEKTOR 11

III. ARCHITEKTUR DER REGISTERLANDSCHAFT NACH DEM ENTWURF DES REGMOG 14

ARCHITEKTUR: 4-CORNER-MODELL UND WEITERE SICHERUNGSMAßNAHMEN 14
VERHINDERUNG UMFASSENDER DIGITALER PERSÖNLICHKEITSPROFILE 15
IDENTIFIKATIONSNUMMER 17
DATENCOCKPIT ALS DATENSCHUTZKONTROLLINSTRUMENT FÜR BÜRGERINNEN UND BÜRGER 18

IV. INTERNATIONALE ARCHITEKTURMODELLE VON REGISTERLANDSCHAFTEN 21

INTERNATIONALE ÜBERSICHT VON REGISTERLANDSCHAFEN 21
KOMBINATION VON SCHUTZMECHANISMEN DER INTERNATIONALEN REGISTERLANDSCHAFTEN 23

Thesen

1. *Eine datenschutzkonforme Registerlandschaft ist eine Grundvoraussetzung für das Erreichen der bestehenden gesetzlich verpflichtenden Digitalisierungsziele des Onlinezugangsgesetzes (OZG) und der europäischen Verordnung zum Single Digital Gateway (SDG-VO).*

   Für das Ziel der gesetzlich verpflichtenden Umsetzung von digitalen Verwaltungsdienstleistung nach OZG[3] und SDG-VO[4] und dem Ziel des elektronischen Zensus sind harmonisierte Register die Grundvoraussetzung. Als harmonisiert gelten Register, wenn ihre Datensätze mit Identifikationsnummern versehen sind, so dass Datensätze über eine Person über fachlich und dezentral gehaltene Register hinweg zweifelsfrei einer Person zugeordnet werden können und übereinstimmen. Dabei wird die Identifikationsnummer zentral verwaltet, während die Inhaltsdaten der jeweiligen Fachmaterie möglichst dezentral bei den zuständigen Behörden gespeichert und verarbeitet werden.

   Der Zugang und die Nutzung der Daten sind - wie bisher - nur mit gesetzlicher Grundlage möglich. Eine vielfach diskutierte Suchfunktion über die fachlich getrennten Register hinweg ist weder vorgesehen noch wäre es aufgrund der logischen Trennung der Register technisch möglich. Die dezentral verteilte Architektur des RegMoG ist im Steuerbereich und Meldewesen entwickelt, erfolgreich etabliert und seit mehreren Jahren im Einsatz.

2. *Zur Verhinderung der Erstellung eines digitalen Persönlichkeitsprofils ist die Sicherung der Datenabfrage bei den Registern entscheidend und nicht das Verbot einer Identifikationsnummer.*

   Bei den historisch nachvollziehbaren Bedenken eines Datenmissbrauches steht insbesondere die personenbezogene Identifikationsnummer in der Kritik. Die Kritik verweist meist auf das Volkszählungsurteil[5], welches in einer Personenkennziffer die Grundlage für eine umfassende Profilbildung gesehen hat.[6] Zudem ist eine Personenkennziffer auch aufgrund historischer und zeitgenössischer Negativbeispiele zu einem Tabubegriff geworden, wie der wissenschaftliche Dienst des Bundestages darlegt.[7] Diese Sichtweise ist jedoch zu kurz gegriffen.[8] Mit den beschränkten Rechenleistungen und den geringen Datenpunkten war das Verbot einer einheitlichen Personenkennziffer 1983 eine wirksame Schutzmaßnahme zur Profilbildung, speziell im thematischen Zusammenhang der Volkszählung.[9] Im 21. Jahrhundert ist fraglich, inwieweit eine Identifikationsnummer als eine notwendige technische Befähigung bewertet werden kann, um digitale Persönlichkeitsprofile zu erstellen. Die umfassende Anzahl an

[3] Onlinezugangsgesetzes (OZG) verpflichtet Bund und Länder ihre Verwaltungsleistungen bis Ende 2022 online anzubieten.
[4] Verordnung (EU) 2018/1724 zum Single Digital Gateway (SDG), bis 12.12.2023 sind 17 Verfahren für Bürgerinnen und Bürger und in 4 Verfahren für die Wirtschaft grenzüberschreitend online zur Verfügung zu stellen, zwingend wenn die Verfahren auch im jeweiligen Mitgliedsstaat angeboten werden; aber auch asymmetrische Verpflichtungen sind denkbar.
[5] BVerfG 15.12.1983, 1 BvR 209/83.
[6] BVerfG 15.12.1983, 1 BvR 209/83, Rn 169.
[7] Deutscher Bundestag – Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes - DSGVO und Recht auf informationelle Selbstbestimmung, bundestag.de/resource/blob/793658/c8c9c4a28cf88a2ae31f81887ec293d9/WD-3-196-20-pdf-data.pdf (07.12.2020).
[8] BVerfG 15.12.1983, 1 BvR 209/83, Rn 152.
[9] *Martini/Wagner/Wenzel,* Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, 38.

Datenpunkten in den staatlichen Registern ist ausreichend, um die überwiegende Mehrheit der Bürger und Bürgerinnen eindeutig zuordnen zu können. In der datenbasierten Verwaltungslandschaft 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 in den durch das RegMoG umfassten Register, eine damit verbundene Ex-Post-Prüfung durch die Bürgerin und den Bürger und einer Ex-Ante-Prüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen mit dem 4-Corner-Modell. Für den Schutz der personenbezogenen Daten in den Registern des RegMoG ist der Zugang zu den Registern entscheidend, nicht das Vorhandensein einer Identifikationsnummer.

3. *Privacy-by-Design durch Separierung der Datenbearbeitung und -speicherung ist ein effektiver Schutz vor einem bundesweiten Datenmissbrauch.*

   Die dezentrale verteilte Speicherung und Bearbeitung der Daten auf Länder- und kommunaler Ebene bedeutet Privacy-by-Design durch Separierung der Daten. Die Verteilung der Datenbestände erzeugt einen höherwertigen Schutz gegen missbräuchliche Zugriffe. Zentrale Register auf Bundesebene wie beispielsweise in Österreich oder Estland haben ein wesentlich höheres Schadenspotential im Fall eines unberechtigten Zugangs und das Angriffsrisiko ist aufgrund der Menge an Daten ebenfalls als wesentlich höher einzustufen. Die vorliegende Architektur folgt der Privacy-by-Design Empfehlung der Europäischen Agentur für Netz- und Informationssicherheit (Separate-Prinzip)[10].

4. *Das 4-Corner-Modell ist aktuell der wirksamste Schutz gegen die Erstellung von digitalen Persönlichkeitsprofilen durch Prüfung der Rechtmäßigkeit vor einer bereichsübergreifenden Übermittlung der Daten.*

   Datenübermittlungen zwischen verschiedenen Bereichen - wie potenziell 'Inneres' und 'Soziales' - werden vor der Übermittlung der Daten auf ihre Zulässigkeit durch das 4-Corner-Modell geprüft (Ex-Ante-Prüfung der Zulässigkeit der Datenabfrage). Zusätzlich werden sowohl durchgeführte als auch abgelehnte Abfragen protokolliert. Die Protokolle sind nicht nur für die Datenschutzbeauftragten zugänglich, sondern sollen zukünftig auch durch die betroffene Person mit Hilfe des Datencockpits überprüfbar gemacht werden. Die Kontrolle der Datennutzung wird damit erheblich erweitert. Das 4-Corner-Modell ist eine europäische Entwicklung zur datenschutzkonformen Übermittlung von Daten, die für die grenzüberschreitende Übermittlung von Daten zwischen EU-Mitgliedsländer über das Single Digital Gateway (SDG) genutzt werden soll.

5. *Das vorgesehene Datencockpit soll nach dem RegMoG-E den betroffenen Personen eine Übersicht über alle Datenübertragungen ermöglichen und eine Datenauskunft zu den Inhaltsdaten nach Art. 15 DSGVO wird empfohlen.*

   Ein zentrales Element in der Gesamtarchitektur des RegMoG ist die Einrichtung eines Datencockpit, welches den betroffenen Personen die Übersicht alle Übermittlungen ihrer persönlichen Daten innerhalb der Registerlandschaft ermöglicht. Diese Protokollierungs-daten werden nicht zentral im Datencockpit gespeichert, sondern weiterhin bei den Quellregistern, die durch die betroffene Person geprüft werden können. Auch bei dieser

[10] ENISA, Privacy by design in Big Data, enisa.europa.eu/publications/big-data-protection/at_download/fullReport (9.12.2020).

Funktion wird das technische Datenschutzprinzip der verteilten Speicherung genutzt. Zusätzlich könnte das Datencockpit den betroffenen Personen auch die Möglichkeit der Auskunft nach der Art. 15 DSGVO über ihre Inhaltsdaten gewährleisten. Die Einsicht in die Protokollierungsdaten und die Inhaltsdaten stärkt maßgeblich den datenschutzrechtlichen Grundsatz der Transparenz nach Art 5 lit a DSGVO, daher wird empfohlen diese Funktionalität explizit im RegMoG vorzusehen.

6. *Die Einführung der Identifikationsnummer kann die Datenschutzgrundsätze nach Art 5 DSGVO maßgeblich stärken.*

   Die aktuelle Datennutzungspraxis im öffentlichen Sektor steht teilweise im Spannungsverhältnis mit den Grundsätzen des Art 5 der Datenschutzgrundverordnung (DSGVO). Aktuelle werden zum Zweck der Identifikation der Person, aufgrund einer fehlenden Identifikationsnummer, zusätzliche personenbezogene Daten (z.B. aktuelle Anschrift, Geburtsdatum und -ort, Mädchenname der Mutter) verarbeitet, gespeichert und zwischen den Behörden übermittelt.[11] Diese Verwaltungspraxis führt zu Datenmaximierung und entspricht nicht dem Grundsatz der Datenminimierung nach Art 5 lit c DSGVO. Aufgrund von Transkriptionsfehlern, Namensverwechslungen, unterschiedlichen Aktualisierungs-frequenzen und verschiedene fachliche Anforderungen besteht dringender Handlungsbedarf die Datenqualität in den Fachregistern zu erhöhen.[12] Die aktuelle Datenqualität in den Registern steht im starken Spannungsverhältnis zum Grundsatz der Richtigkeit und Integrität der Daten nach Art. 5 Abs. 1 lit d DSGVO und führt im Fall von Namensverwechslungen bis zum Bruch der Vertraulichkeit. Die Registerlandschaft und im Besonderen die Identifikationsnummer werden maßgeblich zur Verbesserung der Datenqualität beitragen und somit die Datenschutzgrundsätze nach Art. 5 Abs. 1 lit c und d der DSGVO stärken.

7. *Eine beliebige Kombination von Modellen ist in der Theorie denkbar, in der Praxis zum Scheitern verurteilt.*

   Das durch das RegMoG determinierte Architekturmodell ist komplex in der Zusammenwirkung der ausgewählten Elemente, die in ihrer Kombination den technischen Datenschutz gewährleisten sollen: 4-Corner-Modell, dezentral verteilte Speicherung und Bearbeitung sowie das Datencockpit. Diese Komponenten sind bereits im Einsatz oder im Testbetrieb und bilden daher eine ausgezeichnete Grundlage für eine erfolgreiche Umsetzung. In der Debatte zum RegMoG-E werden unterschiedliche zusätzliche Kombinationen internationaler Modelle diskutiert und vorgeschlagen, beispielsweise eine Mischung der bereichsspezifischen Personenkennzeichen aus dem österreichischen Modell mit dem 4-Corner-Modell und/oder mit einer dezentralen Speicherung. In der Theorie sind diese Modelle eventuell auch kombinierbar, wenn auch nicht immer zweckmäßig oder zielführend. In der Praxis ist aufgrund der steigenden Komplexität des Gesamtsystems eine funktionale Umsetzung eines kombinierten Modells mit einer so hohen Anzahl von Beteiligten von Bund über Länder bis zu den Kommunen fraglich bzw. so gut wie auszuschließen. Dies kann in weiterer Folge auch die Sicherheit aufgrund der steigenden Komplexität des Gesamtsystems reduzieren. Prof. Mertens empfiehlt die Machbarkeit von IT-Großprojekten

[11] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (RegMoG-E), Drucksache 19/24226, 1.
[12] RegMoG-E, Drucksache 19/24226, 1.

im Gesetzesentstehungsprozess als Kriterium zu berücksichtigen, auf Basis seiner Misserfolgsforschung zu gescheiterten IT-Großprojekten in der öffentlichen Verwaltung.[13] Diese Empfehlung ist in Anbetracht der notwendigen datenschutzrechtlichen Abwägungen und der Informationssicherheit von besonderer Bedeutung.

8. Der internationale Vergleich macht sicher.

In der Debatte wird häufig das österreichische Modell mit den bereichsspezifischen Personenkennzeichen (bPK) angeführt, dabei dürfte nicht bekannt sein, dass das bPK-Modell von den Bundesländern aufgrund der hohen Komplexität und eines geringen Mehrwerts nur in wenigen Verfahren genutzt wird. Seit mehr als einem Jahrzehnt fordern die Länder ein bereichsspezifisches Kennzeichen für die Landesverwaltung. Die bPK sind erfolgreich in den Bundesregistern im Einsatz, die allerdings aus Sicht des Datenschutzes den Nachteil der zentralen Speicherung vorweisen. Im direkten internationalen Vergleich ist der datenschutzfreundlichere Weg der dezentralen Speicherung des RegMoG-E hervorzuheben, weder Dänemark, Österreich, noch Estland verfügen über so einen Ansatz. Die Kombination des dezentral verteilten Ansatzes in Kombination mit dem 4-Corner-Modell ist einzigartig und kann weltweit zu einem Vorzeigemodell werden. Neben den technischen Sicherungsmaßnahmen sind auch die rechtlichen Sicherungsmaßnahmen bis hin zum Straftatbestand mit Freiheitsstrafe als führend zu beurteilen.

[13] *Mertens*, Fehlschläge bei IT-Großprojekten der Öffentlichen Verwaltung – ein Beitrag zur Misserfolgsforschung in der Wirtschaftsinformatik, 2008.

I. Nutzen einer harmonisierten Registerlandschaft

Eine harmonisierte Registerlandschaft ist der Schlüssel für eine wirkungsvolle digitale Verwaltung. Dies verdeutlicht auch der Blick zu europäischen E-Government-Spitzenreitern wie Dänemark, Estland und Österreich mit ihren unterschiedlichen Registermodellen (siehe Kapitel IV). Die richtigen Daten mit Vertrauen in ihre Korrektheit bei Bedarf über verschiedene föderale Ebenen und Fachbehörden hinweg abrufen zu können, ist sowohl die Voraussetzung für (halb-)automatisierte Verwaltungsprozesse, holistische Planungsprozesse sowie Analysen und Vorhersagen für die Politikentwicklung.[14]

Datenqualität in der öffentlichen Verwaltung

Korrektes Verwaltungshandeln hängt auch an der Qualität der verfügbaren Daten, sowohl im Einzelfall als auch bei der Planung. Doubletten, veraltete, nicht zuordenbare oder falsch zugeordnete Datensätze erhöhen nicht nur den Prüfaufwand, sondern können sogar zu fehlerhaften Entscheidungen oder der Zustellung an die falsche Person führen. Allein die der öffentlichen Verwaltung vorliegenden Adressdaten sind in über 25 % der Fälle falsch.[15] Dabei können falsch zugestellte Verwaltungsschreiben bis zur Offenlegung vertraulicher Informationen führen. Dies ist insbesondere im Kontext des Grundsatzes der Datenintegrität und Vertraulichkeit der Daten als kritisch zu beurteilen (Art. 5 Abs. 1 lit. f DSGVO).

Mangelhafte Datenqualität kann in aggregierter Form auch leicht zu Fehlplanungen führen, indem etwa Bedarfe über- oder unterschätzt werden. Aufsehenerregend waren beispielsweise die Ergebnisse des registergestützten Zensus 2011, der die amtliche Einwohnerzahl der Bundesrepublik um 1,5 Millionen und Berlins um 180.000 Menschen nach unten korrigierte.[16] Dabei hatte im Vorfeld des Zensus 2011 bereits die Einführung der Steueridentifikationsnummer zu merklichen Korrekturen der Melderegister geführt.[17]

Eine Registerharmonisierung bedeutet durch eine höhere Datenqualität in der Verwaltung also auch weniger fehlerhafte Entscheidungen, eine geringere Wahrscheinlichkeit versehentlicher Datenschutzbrüche und eine bessere Planungsgrundlage.

Eindeutige Daten für (halb-)automatische Verwaltungsprozesse

Routineaufgaben in der Verwaltung zu automatisieren, birgt Zeit- und Kostensparnisse für die Verwaltung sowie für Bürgerinnen und Bürger. Bereits das Zusammensuchen der notwendigen Informationen für die Prüfung eines Antrags beschäftigt schnell Sachbearbeitende in mehreren Behörden und auch die antragstellenden Bürgerinnen und Bürger selbst. Mithilfe eines registerübergreifenden Identitätsmanagements können derartige Prozesse beschleunigt werden, da die für den Antrag relevanten Informationen ohne weiteres menschliches Zutun aus den betreffenden Fachregistern abgefragt werden können.[18] So sehen sich Sachbearbeitende vollständigen Informationsgrundlagen gegenüber.

In einigen Anwendungsfällen können Verwaltungsentscheidungen auch vollautomatisch gefällt werden. Ein einfaches Beispiel hierfür ist die automatische Vergabe von Bewohnerparkausweisen, die

[14] *Thapa/Parycek,* Data Analytics in Politik und Verwaltung in M*ohabbat Kar/Thapa/Parycek*,(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, 40-75.
[15] *Deutsche Post*, „Adress-Studie 2018: Untersuchung zur Qualität von Kundenadressen in Deutschland", 2018.
[16] Statistische Ämter des Bundes und der Länder, Zensus 2011: Zensus Kompakt, 2014.
[17] taz, Neue Steuernummer lässt Berlin schrumpfen, 14.9.2010.
[18] *Mohabbat Kar/Thapa/Hunt/Parycek*, Recht Digital: Maschinenverständlich und automatisierbar - Impuls zur digitalen Vollzugstauglichkeit von Gesetzen", Kompetenzzentrum Öffentliche IT, 2019.

bereits in zahlreichen deutschen Kommunen praktiziert wird.[19] Dabei werden die angegebene Adresse und das Kraftfahrzeugkennzeichen mit dem Melde- und dem Fahrzeughalterregister abgeglichen. In mehr als der Hälfte der Fälle laufen die Anträge vollautomatisch durch das System und die Bürgerinnen und Bürger können sich ihre Bewohnerparkausweise nach Zahlung der Gebühr zuhause ausdrucken. Mangels eindeutiger Identifikationsnummer ist jedoch auch bei der Arbeit mit den bereits bestehenden Registern noch in vielen Fällen menschliches Eingreifen nötig.

Auch die Umsetzung der Grundrente illustriert die Vorteile harmonisierter Registerlandschaften. Bereits die organisationsübergreifende Ermittlung von Lebenspartnerschaften und Einkommen stellt hier eine beachtliche Herausforderung für den digitalen Vollzug dar.[20]

Für (halb-)automatische Verwaltungsprozesse sind Register mit eindeutigen Identifikationsnummern also eine Erfolgsbedingung.

Umsetzung des Once-Only-Prinzips

Das Once-Only-Prinzip ist im E-Government-Aktionsplan der EU 2016-2020[21] verankert und besagt, dass Bürgerinnen und Bürger Informationen der öffentlichen Verwaltung grundsätzlich nur einmal mitteilen sollen.[22] Falls diese Informationen noch an anderer Stelle in der Verwaltung benötigt werden, sollen diese zwischenbehördlich ermittelt werden.

Das Once-Only-Prinzip wird in Deutschland beispielsweise mit der vorausgefüllten Steuererklärung bereits umgesetzt, bei der dem Finanzamt bereits von Arbeitgebern und Sozialversicherungen übermittelte Daten in die Maske der Steuererklärung gespeist werden, so dass Bürgerinnen und Bürger diese Daten nicht ihrerseits bei den zuständigen Stellen erfragen und eintragen müssen.[23]

Bei der Datenerhebung für Verwaltungsverfahren ist der Umweg über Bürgerinnen und Bürger erst dann weitgehend auszuschließen, wenn die relevanten Informationen zuverlässig und in gesicherter Qualität eindeutig zuordenbar in Fachregistern ermittelt werden können. Der vorliegende Gesetzesentwurf ist daher ein wichtiger Schritt zur Umsetzung des Once-Only-Prinzips.

Teilhabewirkung proaktiver Verwaltungsverfahren

Eine automatisierte Anspruchsermittlung kann insbesondere in der Leistungsverwaltung inklusive Wirkung erzielen. So liegt die Nicht-Inanspruchnahme von Sozialleistungen etwa bei Hartz IV bei um die 50 Prozent und bei der Grundsicherung bei ungefähr 60 Prozent.[24] Diese zentralen sozialpolitischen Instrumente erreichen also weniger als die Hälfte der berechtigten Bürgerinnen und Bürger. Als Gründe gelten Unwissenheit über die Anspruchsberechtigung, geringe Ansprüche,

---

[19] Siehe beispielsweise hier: https://ozg.kdn.de/umsetzungsprojekte/details/parkausweise-gesamtprojekt (10.12.2020).

[20] Deutsche Rentenversicherung Bund, Stellungnahme der Deutschen Rentenversicherung Bund anlässlich der Öffentlichen Anhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 25. Mai 2020 zu dem Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung der Grundrente für langjährige Versicherung in der gesetzlichen Rentenversicherung mit unterdurchschnittlichem Einkommen und für weitere Maßnahmen zur Erhöhung der Alterseinkommen (Grundrentengesetz)“, BT-Drucksache 19/18473.

[21] Mitteilung der Kommission COM (2016) 179 final, EU-eGovernment-Aktionsplan 2016-2020.

[22] Bundesministerium für Wirtschaft und Energie, Top 100: Wirtschaft Die wichtigsten und am häufigsten genutzten Verwaltungsleistungen für Unternehmen, 2017, 50.

[23] *Stocksmeier/Wimmer/Führer/Essmeyer*, Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern. Digitalisierung von Staat und Verwaltung, 2019.

[24] *Friedrichsen/Schmacker*, Die Angst vor Stigmatisierung hindert Menschen daran, Transferleistungen in Anspruch zu nehmen, DIW Wochenbericht 26, 2019, 455-461.

Stigmatisierung, insbesondere bei öffentlicher Antragsstellung, und die Komplexität der Inanspruchnahme.[25] Eine proaktive Anspruchsermittlung und folgendes Leistungsangebot an Bürgerinnen und Bürger durch die Verwaltung hätte also eine teilhabe- und sozialpolitisch signifikante Wirkung. Die hierfür nötigen Prüfvorgänge sind ohne harmonisierte Register kaum leistbar.

Antragslose Verfahren

Als besonders bürgerorientiert gelten antragslose Verwaltungsverfahren. In Österreich zeigt die antragslose Familienbeihilfe seit 2015 die Vorteile registergestützter Verfahren. In Deutschland verdeutlicht das Pilotprojekt "Einfach Leistungen für Eltern" (ELFE) die vielen Hürden ohne modernisierte Register.

Österreichische Eltern erhalten anlässlich der Geburt eines Kindes ohne Antrag automatisiert die Familienbeihilfe nach § 10a des Familienlastenausgleichsgesetzes.[26] Nach der Geburt werden die Daten von Kind und Eltern durch das Standesamt im Zentralen Personenstandsregister erfasst und automatisch an Sozialversicherung und Finanzamt weitergeleitet. Liegen alle notwendigen Daten vor, erfolgt mit einem Informationsschreiben über den Familienbeihilfenanspruch an die Eltern gleichzeitig die Überweisung des Familienbeihilfenbeitrags - die Bankverbindung liegt dem Finanzamt meist bereits vor.

Das deutsche ELFE-Projekt will auf ähnliche Weise die Kontaktpunkte der Eltern bei der Gewährung von Familienleistungen reduzieren. Im Idealfall sollen Eltern nur noch ihre Einwilligung für den zwischenbehördlichen Datenaustausch sowie die gewünschte Aufteilung der Elternzeit angeben. Die beteiligten Einrichtungen tauschen die nötigen Daten autonom und digital untereinander aus, bis schlussendlich Urkunden und Leistungen die Eltern erreichen. Mangels harmonisierter Register währen allein die informationstechnischen und rechtlichen Vorbereitungen für das auf Bremen beschränkte Pilotprojekt bereits seit 2018.[27] Erst im November 2020 stimmte der Bundesrat notwendigen Gesetzesänderungen für erste Teilanwendungen von ELFE zu.[28]

Die breite Umsetzung antragsloser Verfahren zum Vorteil der Bürgerinnen und Bürger ist erst mithilfe von harmonisierten Registern und verbindender Identifikationsnummer realistisch.

Registerbasierter Zensus

In einer immer stärker auf Daten basierenden Gesellschaft müssen auch die Grundinformationen höhere Anforderungen erfüllen. Entsprechend plant die Europäische Kommission, ab 2024 jährliche Berichtszeiträume für Bevölkerungszahlen und gegebenenfalls weitere Merkmale wie gewöhnlicher Aufenthalt, Alter oder Geschlecht innerhalb des Europäischen Statistischen Systems.[29] Derart kurze Zensus-Zyklen sind nur mit einem registerbasierten Zensus auf Grundlage einer "verknüpfbaren Registerinfrastruktur" realistisch einzuhalten, wie der Rat für Sozial- und Wirtschaftsdaten

[25] *Buslei,/Geyer/Haan/Harnisch*, Starke Nichtinanspruchnahme von Grundsicherung deutet auf hohe verdeckte Altersarmut, DIW Wochenbericht 49/2019, 909-917.
[26] Familienlastenausgleichsgesetz BGBl 1967/376 idF BGBl I 2019/104.
[27] Freie Hansestadt Bremen "ELFE - Einfach Leistungen für Eltern", https://www.finanzen.bremen.de/digitalisierung/digitalisierungsbuero/elfe einfach leistungen fuer eltern -60128 (10.12.2020)
[28] Gesetz zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen, Bundesrat Drucksache 664/20.
[29] Working Group on Population and Housing Censuses, Post-2020 Census-Strategy, 2014.

empfiehlt.[30] Dabei werden die zensusrelevanten Merkmale in verschiedenen Verwaltungsregistern mithilfe einer einheitliche Identifikationsnummer ermittelt.[31] Hierbei ist ein ”Rückspielverbot” sicherzustellen, also dass der Staat die Daten, die zu statistischen Zwecken erhoben werden, nicht anschließend zum Verwaltungsvollzug verwendet.[32]

Verordnung zum Single Digital Gateway EU (SDG-VO)

Neben den nationalen OZG Zielen bestehen mit der Verordnung zum Single Digital Gateway europarechtliche Verpflichtungen zur grenzüberschreitenden Übermittlung von Registerdaten. Die SDG-VO[33] verpflichtet Mitgliedstaaten zur digitalen Bereitstellung von Verwaltungsverfahren und Hilfsdienste auf eine grenzüberschreitende und diskriminierungsfreie Art und Weise. Grundsätzlicher Maßstab ist die Online-Verfügbarkeit der Verfahren in den jeweiligen EU-Mitgliedsstaaten, der Geburtsnachweis muss jedenfalls mit 12.12.2023 online angeboten werden. Wird ein Verfahren in beiden Mitgliedsstaaten online angeboten, haben beide Mitgliedsstaaten einen digitalen Datentransfer beispielsweise von digitalen Nachweisen aus den jeweiligen nationalen Registern über das Single-Digital-Gateway bis Ende 2023 sicherzustellen. Die Verfahren sind im Anhang 2 der SDG-VO definiert, davon sind 17 Verfahren für Bürgerinnen und Bürger und 4 für die Wirtschaft. Aufgrund der nationalen OZG-Verpflichtung, alle Verwaltungsleistungen bis 2023 online anzubieten, sind diese auch gegenüber EU-Bürgerinnen und -Bürgern online anzubieten und deren digitalen Nachweise über das Single-Digital-Gateway entgegenzunehmen bzw. Nachweise aus Registern von in Deutschland lebenden Personen über das Gateway in andere Mitgliedsstaaten zu transferieren.

Fazit

Ein modernes Registerwesen ist für den Digitalisierungserfolg eines Landes von zentraler Bedeutung. Harmonisierte Register erlauben der Verwaltung die Etablierung vollständig digitaler und zunehmend automatisierter Angebote für Bürgerinnen und Bürger.[34] Erst so werden bürgerfreundliche und effiziente Verfahren wie (halb-)automatische und antragslose Verwaltungsprozesse, die Umsetzung des Once-Only-Prinzips, die Teilhabeeffekte proaktiver Verwaltungsverfahren und die Durchführung registerbasierter Zensus realisierbar. Dabei ist entscheidend, die Datenschutzkonformität der Registerlandschaft bereits durch ihren technischen Aufbau zu sichern. Neben den nationalen Potentialen und rechtlichen Vorgaben des OZG bestehen auch europarechtliche Verpflichtungen durch die SDG-VO, die bereits 2023 erfüllt werden müssen.

[30] Rat für Sozial- und Wirtschaftsdaten, Empfehlungen des RatSWD zum Zensus 2021 und zu späteren Volkszählungen, 2016.
[31] Rat für Sozial- und Wirtschaftsdaten, Empfehlungen des RatSWD zum Zensus 2021 und zu späteren Volkszählungen, 2016, Output, No. 2 (5).
[32] *Martini/Wagner/Wenzel*, 34.
[33] Verordnung (EU) 2018/1724.
[34] *Martini/Wagner/Wenzel,* 42.

II. Datennutzungspraxis im öffentlichen Sektor

Für den Datenschutz gelten in Deutschland die DSGVO, das Bundesdatenschutzgesetz (BDSG) und weitere deutsche Datenschutzregelungen. Maßgebliches Grundrecht ist für den Datenschutz vor allem die informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts.[35] Neben dem diskutierten datenschutzrechtlichen Eingriff durch eine mögliche Einführung einer Identifikationsnummer, ist in einer Gesamtbetrachtung die aktuelle Verwaltungspraxis und das damit verbundene Spannungsverhältnis zu den Datenschutzgrundsätzen nach Art. 5 DSGVO zu berücksichtigen.

Derzeitige Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Datenminimierung

Datenminimierung geht als Grundsatz aus Art 5 Abs 1 lit c DSGVO[36] hervor. Demnach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Personenbezogene Daten sind dem Zweck angemessen, wenn sie der Kontrollfrage 'Sind die Daten erforderlich, um den zuvor festgelegten, eindeutigen Zweck zu erreichen?', standhalten können.[37] Im derzeitigen Verwaltungsalltag werden häufig zusätzliche personenbezogene Daten übermittelt, welche für die eigentliche Aufgabenwahrnehmung nicht notwendig sind. Informationen wie aktuelle Anschrift, Geburtsdatum und -ort sowie der Mädchenname der Mutter dienen ausschließlich der eindeutigen Identifikation, obwohl sie für die eigentliche Aufgabenwahrnehmung nicht notwendig sind.[38] Mit einer solchen unzweckmäßigen Erhebung und Speicherung von Daten, steht die aktuelle Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit c DSGVO.

Ein registerübergreifendes Identitätsmanagement mit einer eindeutigen Identifikationsnummer stellt im Vergleich zur aktuellen Verwaltungspraxis eine erhebliche Verbesserung dar. Dies verdeutlichen die Austauschprozesse zwischen Finanzämtern und beispielsweise den Rentenversicherungen gemäß § 22a Abs. 1 Nr. 1 EStG i.v.m. § 93c Abs. 1 Nr. 2 lit. c AO, wonach einmalig Datensätze ausgetauscht werden, die Folgendes enthalten: den Familiennamen, den Vornamen, den Tag der Geburt, die Anschrift des Steuerpflichtigen und dessen Identifikationsnummer nach § 139 AO. Mit zunehmender Nutzung einer Identifikationsnummer nimmt die Qualität der Daten in den Registern zu, da die Daten aktuell gehalten und regelmäßig berichtigt werden und die übermittelnden Attribute zukünftig noch weiter reduziert werden können. Denkbar und technisch machbar wäre eine Reduktion bis hin zu einem ausschließlich auf die Identifikationsnummer reduzierten Austausch von Daten.

Derzeitige Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Transparenz

Der Grundsatz der Transparenz in Art 5 Abs 1 lit a DSGVO[39] setzt voraus, dass eine bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist.[40] Diese Information kann in elektronischer Form bereitgestellt werden, insbesondere wenn Bürgerinnen und Bürger nur schwer erkennen und nachvollziehen können, ob, von wem und zu

[35] *Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019,1.
[36] Verordnung (EU) 2016/679.
[37] *Paal/Pauly/Frenzel*, DS-GVO[2] Art. 5 Rz 35.
[38] RegMoG-E, Drucksache 19/24226, 1.
[39] Verordnung (EU) 2016/679.
[40] ErwG 58 Verordnung (EU) 2016/679.

welchem Zweck sie betreffende personenbezogene Daten erfasst werden. Gründe dafür können etwa die große Zahl der Datenverarbeitenden oder die Komplexität der benötigten Technik sein.

Da Bürgerinnen und Bürgern nicht dargelegt werden kann, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, steht die aktuelle Verwaltungspraxis im Spannungsverhältnis zum datenschutzrechtlichen Grundsatz der Transparenz. Mit dem im vorliegenden Entwurf geplanten Datencockpit hingegen kann die vorgeschriebene Transparenz umgesetzt werden. Das Datencockpit soll den Bürgerinnen und Bürgern einen Überblick bieten, welche sie betreffenden Datenverarbeitungen wann, durch welche Einrichtung und zu welchem Zweck stattgefunden hat. So wird ein nachträglicher Rechtsschutz möglich. Neben den bestehenden Datenschutzbeauftragten werden so in Zukunft auch die Betroffenen selbst die Kontrolle der Rechtmäßigkeit der Datennutzung stärken.

Mangelnde Richtigkeit und Integrität der Datennutzung in der Verwaltungspraxis

Der Grundsatz der Datenrichtigkeit, wie ihn Art 5 Abs 1 lit[41] festschreibt, kann im derzeitigen System nicht garantiert werden.[42] Die Verarbeitung der personenbezogenen Daten steht im Spannungsverhältnis mit dem Grundsatz der Richtigkeit der Daten nach Art. 5 Abs. 1 lit d DSGVO und im Falle der Weitergabe an Dritte dem Grundsatz der Integrität und Vertraulichkeit Art. 5 Abs. 1 lit. f DSGVO. Derzeit können Personenverwechslungen nicht ausgeschlossen werden, da vorhandene Registerdatensätze den Bürgerinnen und Bürgern nicht immer zweifelsfrei zugeordnet werden können.[43] Aufgrund von Transkriptionsfehlern, Namensverwechslungen, unterschiedlichen Aktualisierungsfrequenzen und verschiedenen fachlichen Anforderungen liegen derzeit in den einzelnen Fachregistern bisweilen mehrere Datensätze zu den gleichen Bürgerinnen und Bürgern vor.[44] Dadurch kommt es zu Trefferlisten, in denen auch die Daten unbeteiligter Personen enthalten sein können, oder zu einem Abbruch des Vorgangs, da die Bürgerinnen und Bürger nicht in allen nötigen Registern auffindbar sind.[45] Eine Identifikationsnummer verhindert derartige Fehler und erhöht somit die Datenqualität sowie die Integrität und Vertraulichkeit durch korrekte Datenweitergabe. Die Identifikationsnummer stellt durch die korrekte Zuordnung von Datensätzen also langfristig die Einhaltung der Grundsätze der Richtigkeit der Daten und der Vertraulichkeit der Daten sicher.

Verwaltung muss Auskunft geben können

Bürgerinnen und Bürger haben laut Art. 15 DSGVO ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten. Um von der Datenverarbeitung Kenntnis zu erlangen und deren Rechtmäßigkeit prüfen zu können, soll das Auskunftsrecht problemlos und in angemessenen Abständen wahrnehmbar sein.[46] Nach enger Auslegung des Begriffs des Verantwortlichen im Sinne der datenverarbeitenden Stelle müsste die betroffene Person hierzu bei der jeweiligen Behörde eine Auskunft der Datenverarbeitung beantragen. Der öffentliche Sektor kann aber auch als eine verantwortliche Stelle auslegt werden, solch einem Auskunftsbegehren kann derzeit nicht nachgekommen werden. Erst der Überblick über alle dem Staat vorliegenden Daten mithilfe der

[41] Verordnung (EU) 2016/679.
[42] RegMoG-E, Drucksache 19/24226, 1.
[43] RegMoG-E, Drucksache 19/24226, 1.
[44] RegMoG-E, Drucksache 19/24226, 1.
[45] RegMoG-E, Drucksache 19/24226, 1.
[46] ErwG 63 Verordnung (EU) 2016/679.

Identifikationsnummer schafft Datensouveränität für Bürgerinnen und Bürger und fördert das Vertrauen in den öffentlichen Sektor.

Datenschutzfreundliche Technikgestaltung (Privacy by Design)

Mit einer datenschutzfreundlichen Technikgestaltung sollen die Grundsätze in Art 5 Abs 1 DSGVO[47], etwa die oben angeführte Datenminimierung, zu einem möglichst frühen Zeitpunkt realisiert werden.[48] Indem von vornherein in geringerem Umfang Daten verarbeitet werden, ist auch das Ausmaß unrechtmäßiger Datenverarbeitungen unwahrscheinlicher.[49] Konkrete Maßnahmen oder Instrumente führt die DSGVO nicht an.[50]

Wie die systematische Umsetzung von Privacy by Design aussehen kann, legt die Europäische Agentur für Netz- und Informationssicherheit (ENISA) in einem Bericht[51] dar.[52] Demnach sollten personenbezogene Daten unter anderem auf ein Minimum reduziert (Minimise) und in getrennten Systemen verarbeitet, ausgewertet und gespeichert werden (Separate). Der vorliegende Entwurf entspricht durch eine Verringerung der für die eindeutige Identifikation notwendigen Attribute - bis hin zur Identifikationsnummer alleine - einerseits dem Minimise-Prinzip. Andererseits folgt die föderal und fachlich verteilte dezentrale Datenverarbeitung und -speicherung dem Separate-Prinzip.

Fazit

Im derzeitigen System werden entgegen dem Grundsatz der Datenminimierung häufig zusätzliche personenbezogene Daten (z.B. aktuelle Anschrift, Geburtsdatum und -ort, Mädchenname der Mutter) nicht für die eigentliche Aufgabenwahrnehmung, sondern ausschließlich zu Zwecken der Identifikation übermittelt.[53]

Die aktuelle Verwaltungspraxis steht im Spannungsverhältnis zum datenschutzrechtlichen Grundsatz der Transparenz, da Bürgerinnen und Bürgern keine Auskunft dazu gegeben werden kann, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden.

Transkriptionsfehler, Namensverwechslungen, unterschiedlichen Aktualisierungsfrequenzen und verschiedene fachliche Anforderungen führen derzeit bisweilen zu Doubletten in den Fachregistern.[54] Dadurch wird dem Grundsatz der Richtigkeit und Integrität der Daten nicht entsprochen.

Ziel der datenschutzfreundlichen Technikgestaltung ist die Umsetzung der datenschutzrechtlichen Grundsätze zu einem möglichst frühen Zeitpunkt. Der vorliegende Entwurf entspricht mit dem Minimise-Prinzip bei der Verringerung der allein für die Identifikation übermittelten Attribute und dem Separate-Prinzip durch dezentrale verteilte Register den durch die Europäische Agentur für Netz- und Informationssicherheit anerkannten Privacy-by-Design-Ansätzen.

---

[47] Verordnung (EU) 2016/679.
[48] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 14.
[49] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 14.
[50] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 17.
[51] ENISA, Privacy by design in Big Data, enisa.europa.eu/publications/big-data-protection/at_download/fullReport (9.12.2020).
[52] *Schütze,* EU: ENISA veröffentlicht Bericht zu Privacy by Design in Big Data, ZD-Aktuell 2016, 05015.
[53] RegMoG-E, Drucksache 19/24226, 1.
[54] RegMoG-E, Drucksache 19/24226, 1.

III. Architektur der Registerlandschaft nach dem Entwurf des RegMoG

Der technische Aufbau des Registermodernisierungsgesetzes strebt einen Ausgleich zwischen den gesellschaftlichen Zielsetzungen, technischen Voraussetzungen und datenschutzrechtlichen Vorgaben an. Das gewählte System zielt dabei auf eine Kombination von verschiedenen Maßnahmen, die unterschiedliche Aspekte des Datenschutzes zum Ziel haben und sich gegenseitig ergänzen.

Die dezentrale verteilte Datenhaltung wird aufrechterhalten und erzeugt weiterhin eine analoge Distanz zwischen den Datenbeständen des Gesamtsystems. Dieser dezentrale Aufbau mit seinen bestehenden Sicherungsmechanismen wird mit dem Gesetz zusätzlich in Bereiche eingeteilt, die bestimmte Datenbestände voneinander trennen. Über das 4-Corner-Modell wird für diese Bereiche eine übergreifende Kommunikation mit hohem Schutzstandart ermöglicht. Zugriffe und Verarbeitungen können auf tatsächlich rechtlich berechtigte Personen und Stellen beschränkt, protokolliert und über ein Portal, dem Datencockpit, den Betroffenen transparent gemacht werden. Das System ermöglicht somit, ex-ante Zugriffe auf einen tatsächlich berechtigten Kreis zu beschränken und ex-post unberechtigte Versuche einer Kontrolle durch die Betroffenen und der Strafverfolgung zu eröffnen. Die zentrale IDNr ermöglicht in diesem System den bereichsübergreifenden Abgleich von Daten und die Transparenz der Verarbeitung. Sie legt den Grundstein für eine digitale Verwaltung. Ihre Einführung wird besonders kritisch gesehen, da nun alle Daten einer Person verknüpfbar sein sollen. Unter Berücksichtigung der Möglichkeiten moderner Datenverarbeitung ist jedoch nicht mehr die theoretische Verknüpfbarkeit ausschlaggebend, diese ist oft schon aufgrund weniger übereinstimmender Datenpunkte möglich, sondern der praktische Zugang. Die im RegMoG-E vorgesehenen Schutzmechanismen, wie Protokollierung der Zugriffe und Zugriffsversuche, Vorabprüfung der Zulässigkeit der Datenübermittlung und dezentraler verteilter Datenhaltung sind zumindest gleichwertig mit bereichsspezifischen Kennzeichen. Diese einzelnen Maßnahmen ließen sich theoretisch noch weiter kombinieren. So entsteht der Eindruck, dass mehr Schichten und Schutzmechanismen auch weiter die Sicherheit steigern, jedoch kann die Sicherheit mit steigender Komplexität auch wieder abnehmen, da eine Kontrolle und Funktionsgarantie des Gesamtsystems immer schwerer zu gewährleisten ist.

In der Gesamtschau legt das Gesetz einen sinnvollen technischen Grundstein für ein zeitgemäßes System der Datenhaltung und Verarbeitung, das traditionelle Anforderungen an den Datenschutz erfüllt und modernen Verarbeitungsmöglichkeiten Rechnung trägt.

Architektur: 4-Corner-Modell und weitere Sicherungsmaßnahmen

Im 4-Corner-Modell werden die Verwaltungsregister nach fachlichen Kriterien in mindestens sechs Bereiche geteilt, wie beispielsweise Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik. Diese Bereiche bilden eine zusätzliche Sicherungsschicht mit Zugriffskontrolle sowie Protokollierung, welche die Datenschutzwirkung der bestehenden dezentralen verteilten Datenhaltung ergänzt. Im Fall einer bereichsübergreifenden Transaktion wird vorab über Intermediäre die Zulässigkeit der Datenabfrage geprüft.

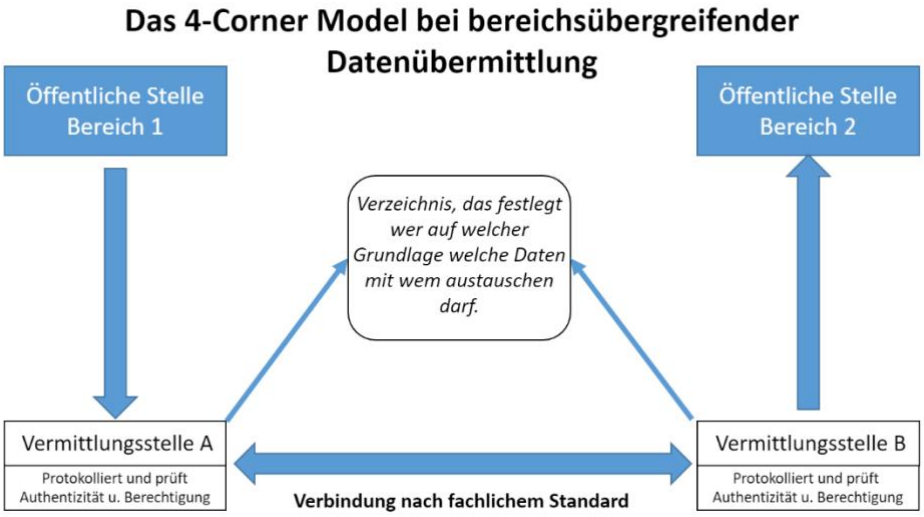
Die bestehenden Standards innerhalb der Bereiche und Bundesländer für Beweissicherung und Revisionsfestigkeit werden nicht geschwächt. Clearingstellen der Länder überwachen bereits die Datenbewegungen unter Einbindung der Datenschutzbeauftragten.[55] Diese Verfahren müssen gem. §

[55] RegMoG-E, Drucksache 19/24226, 51.

7 Abs. 2 S.1 ivm. S. 7 IDNrG-E ebenfalls dem aktuellen Stand von Sicherheit und Technik entsprechen.[56]

Kontrollierte Datenübermittlung

Kernelement des 4-Corner-Modells ist die Kontrolle der Datenübermittlung. So werden Daten im 4-Corner-Modell ausschließlich über neutrale dritte Stellen übertragen. Diese kontrollieren den Zugang und protokollieren die Übermittlung. Im Deutschen Verwaltungsdienstverzeichnis (DVDV) werden die Dienste mit ihren jeweiligen Berechtigungen geführt.[57] So können die Vermittlungsstellen prüfen, welche öffentlichen Stellen auf welcher Rechtsgrundlage miteinander welche Daten austauschen dürfen.



Die Vermittlungsstellen selbst können dabei nicht in die übertragenen Datenpakete hineinschauen, sondern prüfen die Voraussetzungen für den Datenaustausch. Liegen diese Voraussetzungen nicht vor, wird die Anfrage verwehrt und es werden keine personenbezogenen Daten übermittelt. Abfrageversuche mit fehlender Berechtigung oder ohne ein-eindeutige Zuordnung zu einer berechtigten Stelle werden nicht durchgeführt und sind später nachvollziehbar, da sämtliche Datenübermittlungen zwischen öffentlichen Stellen unter Verwendung der IDNr gem. § 9 Abs. 1 IDNrG-E protokolliert werden müssen. Die Datenübermittlungen selbst erfolgen gem. § 7 Abs. 2 IDNrG-E verschlüsselt, nach einem dem aktuellen Stand von Sicherheit und Technik entsprechenden Verfahren. Das genaue Verfahren wird im Rahmen der Vorgaben des § 7 Abs. 2 IDNrG-E durch das gem. § 7 Abs. 2 IDNrG-E BMI in Einvernehmen mit dem Bundesministerium der Finanzen und im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung gem. § 12 Abs. 2 Nr. 6 IDNrG-E bestimmt. Das 4-Corner-Modell wird in der Innenverwaltung bereits eingesetzt und ist auch im IT-Architekturmodell für den EU-weiten Datenaustausch nach der SDG-VO vorgesehen.

Verhinderung umfassender digitaler Persönlichkeitsprofile

Zur Absicherung des Einsatzes einer Identifikationsnummer sind geeignete technisch-organisatorische und rechtliche Mittel entscheidend, wie Martini et al. dargelegt haben.[58] Sie nennen beispielhaft das Risiko einer späteren Profilbildung oder das Risiko für nachhaltige Persönlichkeitsverletzungen bei Schadensfällen. Zur Absicherung dieser Risiken sind mögliche Maßnahmen zu entwickeln, um einem

[56] RegMoG-E, Drucksache 19/24226, 51.
[57] RegMoG-E, Drucksache 19/24226, 51.
[58] *Martini/Wagner/Wenzel*, 44 und 52.

potentiellen Missbrauch vorzubeugen, wie rechtliche Sanktionsmaßnahmen, Maßnahmen zur Datensicherheit, den Datenbestand selbst oder Vorgaben zum Stand der Technik.[59] Das 4-Corner-Modell prüft mithilfe von technischen Prozessen vor der Übermittlung der Daten die Rechtmäßigkeit und sichert zusätzlich mit strafrechtlichen Sanktionen.

In der Gesamtwirkung erscheint das 4-Corner-Modell eine geeignete rechtliche technische Maßnahme darzustellen. Trotz der kombinierten Maßnahmen wird das 4-Corner-Modell als unzureichend kritisiert und bereichsspezifische Identifikationsnummern gefordert. Diese Kritik ist schwer nachvollziehbar, da das Schutzniveau des 4-Corner-Modells mit dem einer bereichsspezifischen Kennziffer als ebenbürtig einzustufen ist bzw. geht es mit der zwingenden Vorabprüfung und Protokollierung noch darüber hinaus. Zusätzlich ermöglicht das Architekturmodell eine dezentral verteilte Führung der Register sowie Kontroll- und Protokollierungsmechanismen, die Datenzugriffe im Gesamtsystem über das Datencockpit transparent und nachverfolgbar machen. Aktuell ist dem AutorInnen-Team keine rechtlich-technische Architektur bekannt, die in ihrer Gesamtwirkung ein ähnlich hohes Schutzniveau vorweisen kann.

Anzahl und Auswahl der Bereiche im 4-Corner-Modell

Damit das 4-Corner-Modell in seiner Schutzfunktion greifen kann, dürfen die einzelnen Bereiche keine Register umfassen, die zu einem Persönlichkeitsprofil verknüpft werden können. Demnach ist zu prüfen, ob das Minimum von sechs Bereichen ausreichend ist. Die tatsächliche Zahl der einzurichtenden Bereiche wird unter Berücksichtigung der jeweils enthaltenen Datenfelder und ihrer Sensibilität festzustellen und der Verordnung gem. § 12 Abs. 1 Nr. 2 IDNrG-E zugrunde zu legen sein.

Zum Teil wird kritisch angemerkt, dass die Einteilung auf Verordnungsebene nach § 12 IDNrG-E problematisch sei. Eine Definition der Bereiche auf Gesetzesebene nähme die Flexibilität gegebenenfalls auch mehr als sechs Bereiche festzulegen, falls dies aus der Perspektive des Datenschutzes notwendig sein sollte. Begrüßenswert wäre es jedoch, eine stärkere, auf Kriterien gestützte Zielsetzung für die Bereichseinteilung in das Gesetz bzw. in die Erläuterungen aufzunehmen. Die vorgeschriebene Mindestzahl von sechs Bereichen deutet bereits an, dass die bestehenden großen Fachbereiche wie Inneres, Justiz, Steuern oder Gesundheit voraussichtlich definiert werden sollen.

Fazit und Ausblick

In der Gesamtschau ist zu beachten, dass das 4-Corner-Modell nicht die einzige Schutzebene ist, die das unberechtigte und unkontrollierte Auslesen und Verknüpfen von Datenbeständen verhindert. Auch innerhalb der Bereiche ist kein beliebiger Datenaustausch möglich. Das 4-Corner-Modell ist bereichsintern zwar nicht verpflichtend vorgeschrieben, kann aber dennoch, wie etwa in der Innenverwaltung bereits zum Einsatz kommen. Ebenso bestehen innerhalb der Bereiche Sicherheitsstandards und Protokollierungspflichten.

Das 4-Corner-Modell ist im Tandem mit dem Datencockpit zu betrachten, auf das noch eingegangen wird. Gemeinsam ermöglichen sie Zugriffskontrollen sowohl ex-ante, indem das Vorliegen der gesetzlichen Zugriffsvoraussetzungen geprüft wird, sowie ex-post durch die Protokollierung der Zugriffsversuche, dadurch wäre erstmals Transparenz der Datenverarbeitung für Bürgerinnen und Bürger garantiert. Darüber hinaus sind über die bestehenden Sanktionsmaßnahmen der DSGVO weitere die Sanktionierung unberechtigter Datenverarbeitungsversuche vorgesehen.

[59] *Martini/Wagner/Wenzel,* 43 ff.

Kern und Stärke der Gesamtarchitektur ist die dezentrale und verteilte Haltung der Inhaltsdaten bei Ländern und Kommunen. Die führenden E-Government-Nationen setzen alle auf zentrale Bundesregister, die ein ungleich höheres Risiko mit sich bringen, weil eine analoge räumliche Trennung fehlt und ein einzelner Angriffsvektor geboten wird.

Identifikationsnummer

Informationelle Selbstbestimmung

Die primäre Kritik am vorgeschlagenen System speist sich aus zwei Befürchtungen: Einerseits die umfassende Profilbildung zu Bürgerinnen und Bürgern mithilfe der Identifikationsnummer, andererseits ein mangelnder Schutz des Systems vor Angriffen von innen oder außen. [60]

Als zentrales Argument in der Debatte gegen die Einführung einer Identifikationsnummer wird das Volkszählungsurteil des Bundesverfassungsgerichts aus 1983 angeführt: [61]

> *„Das Erhebungsprogramm vermag zwar einzelne Lebensbereiche, zum Beispiel den Wohnbereich des Bürgers, jedoch nicht dessen Persönlichkeit abzubilden. Etwas anderes würde nur gelten, soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre; denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig* […]."

Mit den beschränkten Rechenleistungen und spärlichen Datenpunkten der 1980er war das Verbot eines einheitlichen Personenkennzeichens 1983 ein wirksamer Schutz vor Profilbildung. Im 21. Jahrhundert ist ein einheitliches Personenkennzeichen jedoch nicht mehr notwendig, um Datenbestände zu einem Profil zusammenzuführen. Auf Basis der zahlreichen Datenpunkte in Registern und Anwendungen können aktuelle marktübliche IT-Systeme auch ohne eindeutige Identifikationsnummer mit einer hohen Trefferquote zusammengehörige Datensätze zu Personenprofilen bzw. Persönlichkeitsprofilen verbinden.[62] Eine Suche nach Datenpunkten oder eine Verknüpfung von Datenpunkten mit Hilfe der Identifikationsnummer über alle Register ist weder vorgesehen noch aufgrund der logischen Trennung der Register technisch möglich. Eine Profilbildung erfolgt daher nicht über die Identifikationsnummer, sondern über die unrechtmäßige Zusammenführung von Daten zu einer Person. Hierfür muss auf die jeweiligen dezentralen Register und Datenbanken tatsächlich zugegriffen werden können. Dies ist bereits heute nicht der Fall und wird durch die Einführung einer dezentral harmonisierten Registerlandschaft auch nicht ermöglicht. Selbst wenn der Zugang an einem Zugangspunkt kompromittiert wird, kann, aufgrund der dezentralen Struktur nur auf die lokal gespeicherten Daten des jeweiligen Registers zugegriffen werden. Die technischen Voraussetzungen für eine Profilbildung schafft somit nicht erst eine Identifikationsnummer, sondern allein der umfassende Zugriff auf die Register. Entscheidend sind daher die Sicherungsmaßnahmen, die im RegMoG-E vorgesehen sind: Minimierung der

[60] *Kelber*, Stellungnahme des BfDI an den Innenausschuss, bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_InnenA-Registermodernisierungsgesetz.pdf?__blob=publicationFile&v=1 (10.12.2020).
[61] BVerfG 15. 12. 1983, 1 BvR 209/83.
[62] *Martini/Wagner/Wenzel,* 38.

Zugriffsmöglichkeiten durch fachlich und örtlich verteilte Register, revisionssichere Protokollierung aller Zugriffe, eine damit verbundene Ex-Post-Prüfung durch den Bürger und die Bürgerin mit Hilfe des Datencockpits und eine Ex-Ante-Zugriffsberechtigungsprüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen. Die dezentrale verteilte Architektur, die mit dem RegMoG etabliert werden soll, ist auch im internationalen Vergleich eine der Stärken, siehe dazu auch letztes Kapitel.

Steuer-Identifikationsnummer

Die Verwendung der Steuer-Identifikationsnummer als registerübergreifende einheitliche Identifikationsnummer ermöglicht für natürliche Personen die eindeutige Zuordnung in den relevanten Registern der öffentlichen Verwaltung. Dabei kann auf die bereits vorhandenen Strukturen der Steueridentifikationsnummer nach § 139b der Abgabenordnung aufgesetzt werden: So besteht bereits eine Stelle, die den Identifikator fortlaufend betreuen, weiterentwickeln und beaufsichtigen kann. Diese bestehenden Organisationsstrukturen können zeitnah für ein registerübergreifendes Identitätsmanagement aufgerüstet werden.

Derzeit ist die Verwendung der Steuer-Identifikationsnummer auf den steuerlichen Bereich beschränkt. Die Bereiche, in denen die Steuer-ID bereits genutzt wird, reichen von Meldebehörden, Arbeitgebern im Rahmen des Lohnsteuerabzugsverfahrens über Banken, Gerichte und Notare (gemäß § 139b Abs. 2 AO, § 154 Abs. 2a AO, § 93c Abs. 1 Nr. 2 lit. a-c AO, § 26 Abs. 4 u. 5 EGAO, § 22a Abs. 1 Nr. 1 EStG i.v.m. § 93c Abs. 1 Nr. 2 lit. c AO).[63] Die Entwürfe des RegMoG und des IDNrG bauen auf diesen technischen und organisatorischen Erfahrungen auf und stellt damit aus dem Blickwinkel der Informationssicherheit eine geprüfte Grundlage dar.

Registermodernisierungsbehörde

Die nach RegMoG-E einzurichtende Registermodernisierungsbehörde wird keinen dauerhaften Datenbestand aufbauen (vgl. § 11 IDNrG-E). Die Behörde darf nach § 11 IDNrG-E die vom Bundeszentralamt für Steuern übermittelten Basisdaten zum Zweck der Datenübermittlung und Protokollierung zwischenspeichern. Danach sind sie jedoch zu löschen.[64]

Die Basisdaten sind die zur Identifizierung einer natürlichen Person erforderlichen personenbezogenen Daten. Dazu zählen die Identifikationsnummer nach § 139b der Abgabenordnung, Familienname, frühere Namen, Vorname, Doktorgrad, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeiten, gegenwärtige oder letzte bekannte Anschrift, Sterbedatum sowie Tag des Einzugs und des Auszugs.[65]

Datencockpit als Datenschutzkontrollinstrument für Bürgerinnen und Bürger

Das Datencockpit wird in § 10 Abs. 1 OZG als IT-Komponente im Portalverbund beschrieben, in der sich Betroffene Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen, die unter Verwendung der Identifikationsnummer erfolgt sind, anzeigen lassen können. Das Datencockpit fungiert also als Mittler zwischen datenverarbeitenden Stellen und der betroffenen Person. Sinn und

[63] Abgestimmter BLAG-Abschlussbericht, 13.
[64] Deutscher Bundestag - Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 17.
[65] § 4 Abs 2 IDNrG-E.

Zweck des Datencockpits ist, aus dem Zusammenhang des Entwurfs genommen, die Stärkung der informationellen Selbstbestimmung und, aus der Perspektive des BVerfG, die Minderung der Eingriffsintensität. Denn durch den Zugang zu den Protokollen der Datenübermittlung nach § 9 IDNrG können Bürgerinnen und Bürger die Rechtmäßigkeit der Nutzung der sie betreffenden Daten prüfen. So wird eine heimliche Datenverarbeitung erschwert, die für Betroffene grundsätzlich gravierender als eine offene Verarbeitung ist.[66]

Zugang zu und Funktionsweise des Datencockpits

Das Datencockpit soll durch eine noch durch Rechtsverordnung zu bestimmende öffentliche Stelle bereitgestellt werden.[67] Die Registrierung für das Datencockpit hat mit dem Vertrauensniveau "hoch" gem. der eIDAS-VO zu erfolgen. Alternativ sollen Bürgerinnen und Bürger auch ihr Nutzerkonto des Portalverbundes für den Zugang verwenden können.[68] Auch hier ist ein Identifizierungsmittel des Vertrauensniveaus hoch bzw. eines gem. § 3a Abs.2 S.5 VwVfG vorausgesetzt.[69] Ein drei Jahre lang ungenutztes Datencockpit wird automatisch gelöscht. Nutzerinnen und Nutzer können das Konto auch jederzeit selbst löschen und beeinflussen, in welchem Umfang welche Protokolldaten das Datencockpit anzeigen darf.[70] Diese Protokolldaten werden gem. § 10 Abs. 2 OZG nur für jeweils einen Nutzungsvorgang auf den Endgeräten der Nutzerinnen und Nutzer gespeichert. Dauerhaft liegen die Protokolldaten dezentral bei den Registern. Diese sind gemäß § 2 S.1 Nr.3 IDNrG für die Protokollierung zuständig. Vorteil dieses "Quellmodells" ist, dass weder bei den Nutzerinnen und Nutzern noch in einem zentralen Protokollregister eine Ansammlung sensibler Datenbestände entsteht. Dieses Modell lässt sich zeitnah umsetzen und ist offen für einen weiteren Ausbau einer datenschutzkonformen Informationsbereitstellung. Zur Stärkung der Ex-Post-Kontrolle wäre langfristig ein kurzer Beschwerde-/Meldeweg über das Datencockpit bei Zweifeln an der Rechtmäßigkeit einer Datenübermittlung zu begrüßen.

Pflicht der Protokollierung

Die Protokollierungspflicht umfasst nach § 2 S.1 Nr.3 IDNrG-E alle Datenübermittlungen zwischen verschiedenen Rechtsträgern und unterschiedlichen Bereichen. Nach § 9 IDNrG-E sind zudem alle Übermittlungen zwischen öffentlichen Stellen zu protokollieren.

Die Protokolldaten sind gem. § 9 Abs. 3 IDNrG-E zwei Jahre aufzubewahren und anschließend zu löschen. Von der Protokollierung dürften derzeit alle Übermittlungen unter Verwendung der IDNr erfasst sein, da keine Zugangsberechtigungen für nicht-öffentliche Stellen ersichtlich sind. Datenschutzbeauftragte äußerten bereits dahingehende Befürchtungen im Rahmen der Zweckbindung.[71] Sinnvoll wäre daher eine präzise Formulierung der Protokollierungspflichten, sodass sämtliche Datenverarbeitungen und -abrufe auf Grundlage der IDNr zu protokollieren sind. Dies schließt eine mögliche Regulierungslücke.

Protokollierungsstandard

Offen ist nach den Ausführungen im Gesetzentwurf, welche Datenpunkte für die Protokollierung gespeichert werden sollen. § 9 Abs. 1 S. 1 Hs. 2 IDNrG schreibt lediglich eine Weise der Protokollierung

[66] BVerfG 11.03.2008, 1 BvR 2074/05, Rn 79.
[67] § 10 Abs. 5 Neu OZG.
[68] Vgl § 10 Abs. 3 Neu OZG.
[69] RegMoG-E, 128 f.
[70] Vgl § 10 Abs. 4 Neu OZG.
[71] BfDI, Stellungnahme des BfDI zum Entwurf des RegMoG, 6.

vor, die die Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Hierbei entsteht ein Spielraum möglicher gesetzeskonformer Umsetzungen.

Dem Wortlaut von § 12 Abs. 2 Nr. 6 IDNrG-E folgend, besteht eine Verordnungsermächtigung des BMI lediglich für die Ausgestaltung der Protokollierung bei der Registermodernisierungsbehörde, bzw. für Datenübermittlungen zwischen dieser und dem Zentralamt für Steuern.[72] Hier besteht das Risiko, dass sich ein uneinheitlicher Protokollierungsstandard verfestigt, der im Datencockpit zu Darstellungsproblemen führt. Entsprechend ist sicherzustellen, dass die jeweiligen lokalen Protokollierungen vom Datencockpit verarbeitet werden können. Dies sollte mit einer standardisierten technischen Schnittstelle lösbar sein, welche die länderspezifischen Protokollierungen für die standardisierte Abfrage über das Datencockpit übersetzt.

Umfang der Protokollierung

Die Eingriffsintensität des Gesetzentwurfs ergibt sich in Teilen auch aus dem Umfang der Protokollierung. Die Protokollierung muss tatsächlich eine Nachvollziehbarkeit der Verarbeitung ermöglichen. Auch muss die Darstellung im Datencockpit die Nachvollziehbarkeit (Transparenz) der Datenverarbeitung gemäß Art. 5 Abs. 1 lit. a DSGVO sicherstellen. Ebenso sind die Anforderungen an Beweissicherheit und Revisionsfestigkeit zu erfüllen, wobei diese Daten nicht zwingend alle im Datencockpit angezeigt werden müssen, bzw. sollten. Hier ist der Maßstab stärker auf die Nachvollziehbarkeit der Verarbeitung zu setzen und nicht die absolut betrachtete Vollständigkeit aller Protokolldaten.

Zur Beweissicherheit und Revisionsfestigkeit stehen zwei Punkte im Konflikt: Einerseits darf die Protokollierung keine automatisierte Leistungs- und Verhaltenskontrolle der datenverarbeitenden Personen ermöglichen. Andererseits sollte sie möglichst datensparsam eingerichtet werden.[73] Insgesamt sollte auf eine Weise protokolliert werden, die ein Nachvollziehen der einzelnen Verarbeitungsschritte, Anwendungen, Maschinen und Personen mit Zeitbezug erlaubt und diese Daten unveränderlich mit beschränktem Zugang ablegt. Nach § 8 Abs. 2 IDNrG-E ist auf Ebene der Registermodernisierungsbehörde vorgeschrieben, dass durch technische und organisatorische Maßnahmen Daten nicht unbefugt verarbeitet werden können. Ebenso haben abrufende Stellen, die das automatisierte Abrufverfahren nutzen, sicherzustellen, dass nur befugte Personen dieses nutzen können.

Der vorliegende Gesetzesentwurf lässt offen, ob die Protokolle aus Metadaten, Inhaltsdaten oder beidem bestehen. In die Protokolle personenbezogene Inhaltsdaten aufzunehmen, ist nicht empfehlenswert. Metadaten sind für das Nachvollziehen der Datenverarbeitung ausreichend, also beispielsweise Angaben zu Zeitpunkt, Verarbeitungszweck, Verarbeitungsgrundlage sowie der verarbeitenden Stelle. Inhaltsdaten sollten hingegen über das Auskunftsrecht abrufbar sein, die Trennung von Inhaltsdaten und Metadaten ist ein Schutzmechanismus für den Fall einer Kompromittierung des Datencockpits. Das Datencockpit könnte in Zukunft neben der Auskunft über die Datenverarbeitung auch eine Datenauskunft nach Art. 15 DSGVO ermöglichen. Die hier etablierte Infrastruktur könnte ebenso die Grundlage für einen datenschutzkonformen Kontakt zum Staat

[72] Der § 12 Abs. 2 Nr. 6 IDNrG-E nennt explizit nur § 9 Abs. 1 S. 2 IDNrG-E.

[73] Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten der Bundes und der Länder, Orientierungshilfe „Protokollierung, 2009, 3. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2009-OH-Protokollierung.pdf (10.12.2020).

bieten, eine gesetzliche Verankerung einer Funktion zur Datenauskunft nach Art. 15 DSGVO ist empfehlenswert. Zusätzlich sollte ein zukünftiger grenzüberschreitender Datenverkehr nach SDG-VO im Datencockpit abgebildet werden.

IV. Internationale Architekturmodelle von Registerlandschaften

Internationale Übersicht von Registerlandschafen

Im E-Government führende Länder haben funktionierende Registerlandschaften als Basis für digitale Verwaltungsverfahren gemein. Basierend auf der europaweiten Datenschutzdebatte und zur Wahrung der Datensicherheit besitzen diese Registerlandschaften Schutzmechanismen, um Datenmissbrauch zu verhindern.

Schutzmechanismen	**Deutschland (RegMoG)**	**Österreich**	**Estland**	**Dänemark**
System bereichsspezifischer Personenkennzeichen	-	x	-	-
Ex-Ante-Berechtigungsprüfung durch Intermediär (4 Corner)	x	(x) auf Bundesebene	x	x
Ex-Post Kontrollierbarkeit der Datenzugriffe, Datencockpit	x	(x) teilweise in Planung	x	-
Dezentrale verteilte Register	x	-	-	-
Datenschutz als Verfassungsrecht, strenge Datenschutzaufsicht, Evaluierung und Berichtswesen ans Parlament, Straftatbestand mit Freiheitsstrafe	x	-	-	-

[74]

Österreich

In der Debatte wird häufig das österreichische Modell und die bereichsspezifischen Personenkennzeichen (bPK), die aus Stammzahlen gebildet werden, als eine der wirksamsten datenschutzrechtlichen Maßnahmen angeführt. In Österreich kann die Stammzahl als allgemeines Personenkennzeichen gewertet werden.[75] Allerdings ist die Stammzahl nur der Stammzahlenregisterbehörde bekannt, sie wird nicht zwischen den Behörden übermittelt und damit nicht verbreitet.[76] Mit der Einführung der Kombination aus Stammzahl und bPK wird grundsätzlich eine grundrechtsschonende Lösung gewählt und dem Gedanken “Privacy by Design” Rechnung getragen, da die Möglichkeiten von Datenabfragen und Zusammenführungen nicht erweitert werden.[77] Allerdings wird die fortlaufend notwendige bPK-Berechnung für Datenübermittlungen an einer zentralen Stelle vorgenommen, sodass theoretisch die Gefahr der Datensammlung an der sensiblen Stelle besteht. In Diskussion ist eine Verschlüsselung der Inhaltsdaten und der Protokolldaten.

[74] Vgl Stellungnahme Nationaler Normenkontrollrat (NKR), 12/2020.
[75] *Martini/Wagner/Wenzel*, 38.
[76] *Martini/Wagner/Wenzel*, 38.
[77] *Martini/Wagner/Wenzel,* 40.

Das bPK-System wurde Anfang 2000 entwickelt und auf Bundesebene in mehr als 30 Registern realisiert, die Daten werden, selbst wenn lokale Register vorliegen, zentrale auf Bundesebene harmonisiert, gespeichert und verarbeitet. Das Angriffs- und Missbrauchsrisiko beim österreichischen Zentralen-Melderegister (ZMR) ist im Vergleich zur aktuellen dezentral verteilten Lösung des deutschen Meldewesens höher einzustufen. Im Fall eines unberechtigten Zugangs oder eines Missbrauchs durch Zugangsberechtigte kann im österreichischen Melderegister grundsätzlich auf alle Daten zugegriffen werden. In Deutschland ist im gleichen Fall nur das jeweilige lokale Melderegister betroffen, das nur einen Ausschnitt der Meldedaten enthält. Das Risiko wurde beim österreichischen Ergänzungsregister für Sonderfälle natürlicher und juristischer Personen sichtbar, bei welchem über Jahre persönliche Daten von mindestens einer Million Bürger und Bürgerinnen öffentlich zugänglich waren.[78]

Das österreichische System bietet keine Kontrollfunktion der Datennutzung. Ein Zugriff auf die Protokolldaten durch die betroffene Person ist nicht vorgesehen. Geplant ist hingegen die Weitergabe von staatlichen Daten durch Bürgerinnen und Bürger an die Wirtschaft. Durch die dazu notwendigen bPK-Berechnungen sind die Metadaten der Datentransaktionen während der Transaktion bzw. im Anschluss theoretisch in einem dafür vorgesehenen Datencockpit einsehbar. Der Fokus liegt dabei auf die Protokollierung der Datenübermittlung, die durch den Bürger oder die Bürgerin initiiert wurde. Ein zukünftiger Vorteil des österreichischen Datencockpits wird ein automatisiertes Auskunftsrecht über die bPK-geführten Register. Nicht dazu zählen aufgrund der fehlenden Ausstattung mit bereichsspezifischen Personenkennzeichen die Register und Datenanwendungen auf der Landesebene. Die Landesverwaltungen, die um ein Vielfaches mehr Verfahren führen, haben die bPK nicht oder nur für vereinzelte Verfahren eingeführt. Dadurch mangelt es an der durchgehend praktischen Umsetzung und Wirkung des Systems, trotz einer Einführung vor über 15 Jahren.

Estland

Das X-Road-System in Estland ermöglicht den Datenaustausch zwischen autorisierten Datenbanken, wobei streng geregelt ist, wer was speichern und worauf zugreifen darf. Ähnlich dem 4-Corner-Modell erfolgt eine Ex-Ante-Prüfung. Daten werden zum überwiegenden Teil auf nationaler Ebene gespeichert. Gemeinsamer Grundsatz ist, dass die Daten dort gespeichert werden, wo sie entstehen.[79] Bürgerinnen und Bürger können auf all ihre Inhaltsdaten zugreifen und diese auch für von ihnen verantwortete Prozesse nutzen. Zusätzlich können Bürgerinnen und Bürger ex-post nachvollziehen, wer die Daten wann verarbeitet hat. Zur Harmonisierung der Daten wird wie im RegMoG-E eine Identifikationsnummer in den Registern geführt.

Dänemark

In Dänemark werden von Behörden die Basisdaten, zum Beispiel Informationen über Personen, Unternehmen oder Orte, registriert und im gesamten öffentlichen Sektor wiederverwendet.[80] Die Basisdaten müssen zuverlässig und von hoher Qualität sein. Um Behörden, Unternehmen und Bürgerinnen und Bürgern einen leichten Zugang zu den Daten zu ermöglichen, sind sie über den ”Data Distributor” teilweise frei zugänglich.[81]

---

[78] https://epicenter.works/content/groesster-datenskandal-der-republik-ueber-eine-million-wohnadressen-oeffentlich (10.12.2020).
[79] https://thedigitalarchitects.de/x-road-estland/ (10.12.2020).
[80] The Danish Government/Local Government Denmark, Good basic data for everyone – a driver for growth and efficiency, 2012.
[81] The Government/Local Government Denmark/Danish Regions: A stronger and more secure digital Denmark, Digital Strategy 2016-2020, 2016.

Kombination von Schutzmechanismen der internationalen Registerlandschaften

In den aktuellen Gutachten und Stellungnahmen zum RegMoG-E wird eine Kombination von Schutzmechanismen der beschriebenen internationalen Modelle vorgeschlagen. Beispielswiese eine Mischung der bereichsspezifischen Personenkennzeichen aus dem österreichischen Modell mit dem 4-Corner-Modell und/oder mit einer dezentralen Speicherung. In der Theorie sind diese Modelle kombinierbar, wenn auch nicht immer zweckmäßig. In der Praxis ist aufgrund der steigenden Komplexität des Gesamtsystems eine erfolgreiche Umsetzung von kombinierten Schutzmechanismen so gut wie auszuschließen. Der Vorschlag, das österreichische bereichsspezifische Kennzahlsystem mit dem Modell einer dezentralen verteilen Datenhaltung und -verarbeitung des deutschen RegMoG-E zu kombinieren, übersteigt in seiner technischen und seiner organisatorischen Komplexität angesichts der föderal verteilten Organisationen des Bundes, der Länder und der Kommunen eine Schwelle der Machbarkeit. Eine dadurch verzögerte Umsetzung hätte zum Ergebnis, dass die aktuellen datenschutzrechtlichen Spannungsfelder der Datenminimierung, Transparenz und Datenintegrität über das nächste Jahrzehnt nicht auflösbar wären. In Folge wären auch die Ziele des Gesetzes nicht erreichbar, weil eine datenschutzkonforme Registerlandschaft die Grundlage sowohl für digitale Verwaltungsverfahren in Deutschland als auch für die europarechtlich zwingend vorgesehenen grenzüberschreitende Verwaltungsverfahren bildet.

Eine andere diskutierte Variante sind zentrale Register nach dem österreichischen Modell. Die dezentrale Registerstruktur in Deutschland - im Gegensatz zur zentralen Struktur in Österreich - müsste unter großem Aufwand zurückgebaut und die gesamte etablierte Datenkommunikation reorganisiert werden.[82] Technisch wäre dieses Vorgehen mit großem finanziellem und zeitlichem Aufwand möglich. Die Speicherung der fachlichen Daten auf Bundesebene löst jedoch das Privacy-by-Design-Prinzip der Separierung der Daten durch dezentrale lokale Speicherung auf und verliert so eine zentrale Stärke des RegMoG-E auf. Durch die zentrale Speicherung und Verarbeitung wäre zwar das bPK-Modell anwendbar, aber die Motivation für Angriffe und das Datenmissbrauchspotential generell würden dadurch steigen. Aufgrund der wesentlich höheren Komplexität des Architekturmodells, der hohen Anzahl der Beteiligten und der fehlenden Erfahrungen mit den bPK-Komponenten ist eine erfolgreiche und vor allem zeitnahe Umsetzung bis Ende 2023 so gut wie auszuschließen.

In Abwägung dieser beiden Modelle ist die vorgeschlagene Architektur des RegMoG-E mit dezentraler verteilter Speicherung und Verarbeitung, der Vorabprüfung (ex-ante) der bereichsübergreifenden Kommunikation durch das 4-Corner-Modell und einer nachträglichen Prüfung der Protokolldaten durch die Bürgerinnen und Bürger (ex-post) nach Einschätzung des AutorInnen-Teams eine größere Stärkung der informationellen Selbstbestimmung und somit ist auch aus der Perspektive des Datenschutzes dem RegMoG-E im Vergleich zu anderen Varianten der Vorzug zu geben.

[82] Deutscher Bundestag - Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 11.