ID Austria
Datenschutz-Folgenabschätzung

Research Institute – Digital Human Rights Center

ID Austria

Datenschutz-Folgenabschätzung

Bericht zur Datenschutz-Folgenabschätzung der ID Austria im Auftrag des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW)

Wien, Mai 2022

Autoren:
Christof Tschohl
Moritz W. Rothmund-Burgwall
Robert Rothmann
Markus Kastelitz
Jan Hospes
Philipp Poindl
Walter Hötzendorfer

Research Institute – Digital Human Rights Center
smart.rights.consulting

IMPRESSUM

Medieninhaberin und Herausgeberin:
Research Institute AG & Co KG
FB-Nr.: 355966f, HG Wien
Amundsenstraße 9, 1170 Wien

Das Research Institute (RI) ist eine unabhängige Forschungseinrichtung
an der Schnittstelle von Technik, Recht und Gesellschaft.
Die Tätigkeiten des Institutes umfassen wissenschaftliche Forschung
und Lehre sowie Consulting.

Web: https://researchinstitute.at
E-Mail: office@researchinstitute.at
Twitter: @researchinst

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	15.03.2022	V 0.9	Konsolidierung der DSFA	Christof Tschohl	prä-finale Version
2	25.04.2022	V 1.0	Lektorat Gesamtdokument, Management-Summary	Christof Tschohl	finale Version

Disclaimer

Sofern im Folgenden nicht anders angegeben, wurden alle Internetlinks zuletzt am 22. 04. 2022 abgerufen.

Im Sinne eines diskriminierungsfreien Sprachgebrauchs ist der vorliegende Bericht mit * gegendert. Da einschlägige Gesetzestexte mitunter das generische Maskulinum verwenden, sind gesetzlich definierte Fachtermini wie zB der *Verantwortliche*, oder der *Auftragsverarbeiter* kursiv gesetzt. Bezeichnungen aus dem Englischen, wie zB Service Provider oder User, werden in ursprünglicher Form verwendet.

Inhaltsverzeichnis

1 Management Summary 1

2 Einleitung 4

2.1 Erforderlichkeit einer Datenschutz-Folgenabschätzung (Schwellenwertanalyse) 6

3 Sachverhaltsdarstellung und Spezifizierung des Prüfgegenstands 13

3.1 Technische Architektur der ID Austria 15

3.2 Datenverarbeitungstätigkeiten im ID Austria System 20

3.2.1 Registrierung und Akkreditierung der Service Provider 20

3.2.1.1 Registrierung 21

3.2.1.2 Akkreditierung 28

3.2.2 Registrierung der Benutzer*innen 31

3.2.2.1 Architekturüberblick des E-ID-Registrierungsprozesses 32

3.2.2.2 Registrierungsprozess 32

3.2.2.3 Registrierungsvarianten 35

3.2.3 Verwendung der ID Austria 42

3.2.3.1 Erstellung einer qualifizierten elektronischen Signatur 42

3.2.3.2 Binding-Erstellung 43

3.2.3.3 Anmeldung an Service Provider 44

3.2.4 Verwaltung des E-ID über „Meine ID Austria“ 49

4 Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge 52

4.1 Was sind personenbezogene Daten? 53

4.1.1 Datenstrukturen und eindeutige Identifikatoren im ID Austria System 55

4.2 Rechtsgrundlagen 60

4.2.1 Regelungssystematik der DSGVO 60

4.2.2 Datenverarbeitung zum Zwecke der Registrierung und Akkreditierung privater Service Provider 61

4.2.3 Datenverarbeitung zum Zweck der Registrierung der Benutzer*innen 62

4.2.4 Datenverarbeitung zum Zweck der Verwendung der ID Austria 64

4.2.5 Datenverarbeitung zum Zweck der Verwaltung des E-ID über „Meine ID Austria“ 67

4.3 Rollenverteilung nach Maßgabe der DSGVO 69

4.3.1 Allgemeine Systematik der Rollenverteilung 69

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) *Verantwortlichen* 73

4.3.3 Rollenverteilung im E-ID Gesamtsystem 74

4.3.3.1 Registrierung und Akkreditierung privater Service Provider 76

4.3.3.2 Registrierung der Benutzer*innen 76
4.3.3.3 Verwendung des E-ID 80
4.3.3.4 Verwaltung des E-ID über „Meine ID Austria“ 82
4.4 Angaben über Maßnahmen zur Einhaltung der DSGVO 83
4.4.1 Grundsatz der Zweckbindung 83
4.4.2 Grundsatz der Datenminimierung 84
4.4.3 Grundsatz der Speicherbegrenzung 86
4.5 Angaben über die Berücksichtigung der Betroffenenrechte 88
4.5.1 Gewährleistung der Transparenz und Informationspflichten 88
4.5.2 Recht auf Auskunft und Datenübertragbarkeit 88
4.5.3 Recht auf Berichtigung und Löschung 88
4.5.4 Recht auf Einschränkung und Recht auf Widerspruch 89
4.5.5 Recht auf Beschwerde 91
4.6 Datenschutzrechtliche Anforderungen an die Protokollierung 92
4.6.1 Was versteht man unter „Protokollierung“? 94
4.6.2 Inhalt von Protokolldaten 95
4.6.3 Wozu wird protokolliert? 95
4.6.4 Auswertung von Protokollen 96
4.6.5 Wie lange dürfen Protokolle aufbewahrt werden? 97
4.6.6 Exkurs: Auskunftsrecht der betroffenen Personen 98
4.6.7 Umsetzungsstrategie zur Protokollierung im Rahmen der ID Austria 99
4.6.7.1 Umsetzung der Protokollierung 99
4.6.7.2 Zur Geltungs- und Speicherdauer von Einwilligungen 101
4.6.7.3 Auswahl geeigneter technischer und organisatorischer Maßnahmen 103
4.7 Datenübermittlung an Drittländer (oder internationale Organisationen) 106
4.8 Rat des *Datenschutzbeauftragten* und Standpunkt der Betroffenen 109
5 Datenschutzrechtliche Risikoabschätzung – Risk Assessment 115
5.1 Methodologie 117
5.2 Risikobeurteilung 126
5.2.1 Unbeabsichtigte Erstellung eines E-ID 126
5.2.2 Sozialer Druck zur Erstellung bzw Nutzung des E-ID 128
5.2.3 Staatliche Infrastruktur mit Überwachungspotenzial 130
5.2.4 Rechtswidriger Zugriff auf Protokolldateien der Anmeldehistorie 133
5.2.5 Rechtswidriger Zugriff auf Protokolldateien der Identity Provider 135

5.2.6 Nichtverfügbarkeit des Systems aufgrund fehlgeschlagener Authentifizierung 137
5.2.7 Unbefugte Verarbeitung biometrischer Daten 139
5.2.8 Gewaltanwendung zur Erlangung des zweiten Faktors 141
5.2.9 Identitätsdiebstahl durch Kompromittierung der biometrischen Absicherung 143
5.2.10 Identitätsdiebstahl durch Unterschieben eines biometrischen Merkmals 146
5.2.11 Identitätsdiebstahl durch mangelnde Sicherheit der Anmeldung 148
5.2.12 Identitätsdiebstahl durch strukturelle Schwächen des Konzepts Passwort 150
5.2.13 Mangelhafte Akkreditierung behördlicher Service Owner bzw Provider 152
5.2.14 Zweckwidrige Verarbeitung durch Service Owner 154
5.2.15 Zweckwidrige Zusammenführung von Attributen 156
5.2.16 Rechtswidrige Verarbeitung durch die systembetreibenden Verantwortlichen 158
5.2.17 Intransparenz der Datenverarbeitung im Rahmen des E-ID Systems 160
5.2.18 Unbewusste oder irrtümliche Datenherausgabe 162
5.2.19 Abhängigkeit in der Nutzung der Ökosysteme von Google und Apple 164
5.2.20 Zweckwidrige Verarbeitung durch Firebase Cloud Messaging 166
5.3 Diskussion der verbleibenden Risiken und Folgenabschätzung 168
6 Fazit und getroffene Entscheidungen 170
6.1 Ausblick 170
6.2 Pflicht zur künftigen Überprüfung 171
Glossar und Abkürzungsverzeichnis 172

1 Management Summary

Der vorliegende Bericht dokumentiert die Ergebnisse der Datenschutz-Folgenabschätzung (DSFA) zum Einsatz des ID Austria Systems als österreichische Variante eines elektronischen Identitätsnachweises (E-ID). Dabei ist ein elektronischer Identitätsnachweis (E-ID) gemäß § 2 Z 10 E-Government-Gesetz rechtlich definiert als eine logische Einheit, die eine qualifizierte elektronische Signatur mit einer Personenbindung und den zugehörigen Sicherheitsdaten und -funktionen verbindet. Als solche soll die ID Austria in der Online-Welt künftig als digitaler Nachweis der persönlichen Identität dienen. Sie bietet die Möglichkeit zur Authentifizierung gegenüber einer Reihe an Diensten und Anwendungen aus dem behördlichen und privaten Sektor.

Bei der technischen Entwicklung und (europaweiten) Implementierung des E-ID handelt es sich somit um eine bedeutende Infrastruktur der Informationsgesellschaft, welcher in der künftigen Anwendung ein erhebliches Potential für die Bürger*innen und Nutzer*innen zugesprochen wird. Zugleich gehen damit eine Reihe an potenziellen datenschutzrechtlichen Risiken einher, welche die Durchführung einer DSFA aus verschiedenen Gründen erforderlich machen. So kommt es im Rahmen der geplanten Anwendung jedenfalls zur Verarbeitung eines großen Umfangs an personenbezogenen Daten, der vorliegende Bericht analysiert daher diese Verarbeitung im Detail und bewertet sie in datenschutzrechtlicher Hinsicht.

Aufgrund des spezifischen Zwecks des E-ID Systems kann es weiters auch zu Fällen kommen, in denen das Funktionieren der ID Austria für Betroffene eine wesentliche Grundlage für die Ausübung ihrer Rechte oder die Inanspruchnahme von Dienstleistungen darstellt.

In der methodischen Umsetzung und Durchführung der Datenschutz-Folgenabschätzung wurde im Sachverhalt auf die folgenden Datenverarbeitungsprozesse fokussiert:

- die Registrierung und Akkreditierung behördlicher und privater Service Provider;
- die Registrierung der Benutzer*innen;
- die Verwendung der ID Austria durch die Benutzer*innen nach erfolgter Registrierung;
- die Verwaltung der ID Austria durch die Benutzer*innen (Funktion „Meine ID Austria“).

Zudem wurde in der Analyse besonderes Augenmerk auf die datenschutzrechtliche Rollenverteilung und Verantwortlichkeit innerhalb der verschiedenen Datenverarbeitungsprozesse gelegt. Die mit der technischen Architektur des Systems einhergehende Frage der Protokollierung von Transaktions-Logs wurde ebenfalls ausführlich und kritisch behandelt.

Im Kern der DSFA werden zahlreiche datenschutzrechtliche Risiken in methodisch systematischer Weise analysiert und anhand einer quantitativen Matrize beurteilt. Dabei wird beispielsweise die Frage der Freiwilligkeit der Nutzung des E-ID Systems ebenso abgehandelt wie verschiedene Formen möglicher zweckwidriger Verarbeitung oder Varianten des Identitätsdiebstahls. Die Risikobeurteilung geht nicht zuletzt auch auf die Thematik des Potenzials zur Überwachung ein und greift das Thema einer möglichen Intransparenz der Datenverarbeitung auf.

In der Analyse zeigt sich, dass von Seiten der Verantwortlichen ab der ersten Planung des Systems zahlreiche technische und organisatorische Maßnahmen ergriffen wurden, um die Risiken zu mitigieren und die Einhaltung der Grundsätze des Datenschutzrechts zu gewährleisten.

Auf Basis der im Rahmen der vorliegenden DSFA durchgeführten Risikobeurteilung kann festgehalten werden, dass die identifizierten Risiken aufgrund der gesetzten Maßnahmen für die Betroffenen im Produkt ihrer Eintrittswahrscheinlichkeit und Schwere nicht als hoch einzustufen sind und somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Artikel 36 DSGVO besteht. Die Notwendigkeit und Verhältnismäßigkeit der untersuchten Datenverarbeitungsprozesse werden auf Basis einer entsprechenden systematischen Analyse in Verbindung mit den Rechtsgrundlagen und unter Berücksichtigung aller technischen und organisatorischen Maßnahmen als gegeben erachtet.

Als Ergebnis dieses sorgfältig durchgeführten Analyseprozesses kann zusammenfassend festgehalten werden, dass

- bereits die Architektur des ID Austria Systems dem „Privacy by Design“ Prinzip des Datenschutzrechts und damit auch dem Grundsatz der Datenminimierung folgt;
- die Protokollierung hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt ist;
- personenbezogene Daten stringenten Pseudonymisierungs- und Löschfristen unterliegen;
- personenbezogene Daten nur von berechtigten Stellen verarbeitet bzw übermittelt werden, soweit diese hierfür notwendig sind
- gespeicherte personenbezogene Daten strengen Zugriffsrechten unterliegen;
- nur die für die Zweckerfüllung erforderlichen Daten erhoben werden bzw sind im Registrierungs- und Anmeldeprozess nur Felder und Funktionen vorgesehen, die erforderlich sind.

Nichtsdestotrotz gilt es die weitere technische, rechtliche und gesellschaftliche Entwicklung sorgfältig zu beobachten und die Auswirkung auf die Rechte und Freiheiten der Betroffenen laufend zu prüfen. Dabei ist neben einer zweckwidrigen oder unverhältnismäßigen Anwendung des staatlichen ID Systems insb auf Formen der Diskriminierung und Ungleichbehandlung zu achten. In diesem Sinne betrachtet die DSFA nicht nur die Risiken für die Rechte und Freiheiten einzelner Individuen, sondern wahrt auch den Blick auf die gesamte Gesellschaft.

Darüber hinaus sind auch technische und internationale Weiterentwicklungen zur Implementierung und weiteren Optimierung von E-ID Architekturen im Lichte des „Privacy by Design“ Konzepts zu beobachten. An dieser Stelle ist festzuhalten, dass die einzelnen Anwendungen, die nun künftig an die Infrastruktur der ID Austria andocken, für sich genommen ebenfalls alle datenschutzrechtlichen Anforderungen erfüllen müssen und insbesondere den Grundsatz „Datenschutz durch Technikgestaltung und Voreinstellungen“ zu wahren haben. Das BMDW als *Verantwortlicher* wird dazu – zeitnah zum offiziellen Start der ID Austria – auch den Bericht über die Datenschutz-Folgenabschätzung zum „Digitalen Führerschein“ veröffentlichen, dem ersten Pionierprojekt im Rahmen der geplanten „Digitalen Ausweisplattform“.

Schließlich trifft den *Verantwortlichen* eine aktive Monitoring-Verpflichtung im Hinblick auf alle für das System relevanten tatsächlichen oder rechtlichen Umstände. Lassen sich wesentliche Änderungen in der Risikolage identifizieren, sind jedenfalls angemessene technische und organisatorische Anpassungen der Maßnahmen für eine datenschutzkonforme Verarbeitung der personenbezogenen Daten vorzunehmen. Diese notwendige ständige Weiterentwicklung kennt keine Pause, so wird bereits während des offiziellen Starts der ID Austria (nach dem Ablauf der Pilotphase) bereits an

weiteren Optimierungen gearbeitet, die zeitnahe umgesetzt werden. Das wichtigste Beispiel hierfür ist die Umsetzung eines Token-Systems als Alternative zu den biometrischen Identifizierungsverfahren.

Die Datenschutz-Folgenabschätzung selbst ist, wie auch dieser Bericht, ein lebendiges Instrument, welches fortlaufend durch den *Verantwortlichen* zu pflegen und weiterzuentwickeln ist. Die dafür erforderliche Dynamik in den Prozessen des *Verantwortlichen* wird durch dessen Datenschutz-Management System sichergestellt und zugleich durch einen offenen und sachlichen gesellschaftlichen Diskurs befördert. Der hier vorliegende konsolidierte Bericht und dessen Veröffentlichung soll in diesem Sinne Transparenz schaffen und einen wesentlichen Beitrag dazu leisten.

Der DSFA-Bericht gelangt somit zu dem Ergebnis, dass es im ID Austria System eine Vielzahl an Garantien und Verfahren gibt, welche die potentiellen Risiken der geplanten Verarbeitungsprozesse eindämmen sowie den Schutz personenbezogener Daten sicherstellen. Die Einhaltung aller datenschutzrechtlichen Anforderungen und Bestimmungen ist gewährleistet und wird durch diesen Bericht dokumentiert.

2 Einleitung

Der vorliegende Bericht dokumentiert die Ergebnisse der durchgeführten Datenschutz-Folgenabschätzung (DSFA) zur ID Austria als österreichische Variante des elektronischen Identitätsnachweises (E-ID) zur Identifikation von Bürger*innen gegenüber digitalen Anwendungen und Diensten aus dem behördlichen und privaten Umfeld. Der Bericht dient insbesondere der Prüfung der damit verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung ihrer personenbezogenen Daten. Zudem ist der vorliegende Bericht (neben der sonstigen Datenschutz-Dokumentation) als Nachweis der Einhaltung der Grundsätze des Datenschutzrechts – insb der Rechenschaftspflicht des Verantwortlichen gem Art 5 Abs 2 der Datenschutz-Grundverordnung (DSGVO) – zu verstehen.[1] Als solcher adressiert er insb die interessierte Öffentlichkeit; gegebenenfalls erfolgt eine Vorlage an den Datenschutzrat sowie an die österreichische Datenschutzbehörde.

Aus organisatorischer Sicht ist eingangs festzuhalten, dass die Durchführung einer DSFA grundsätzlich der für die Datenverarbeitung verantwortlichen Stelle selbst obliegt. Als datenschutzrechtlich *Verantwortlicher* hat das *Bundesministerium für Digitalisierung und Wirtschaftsstandort* (BMDW) das *Research Institute – Digital Human Rights Center* (RI) im Herbst 2021 mit der Unterstützung in der Ausarbeitung der vorliegenden Dokumentation zur DSFA beauftragt. Die Beiziehung des RI als externes Beratungsunternehmen stellt daher keine gänzliche Auslagerung, sondern vielmehr eine wesentliche fachliche Unterstützung in der Umsetzung der Datenschutz-Folgenabschätzung dar. Zudem liegen viele der für die Durchführung der DSFA benötigten Informationen primär in der Sphäre des *Verantwortlichen* und sind auf Grund der agilen Projektentwicklungsmethode nicht immer zentral gesammelt und aufgezeichnet, sondern mitunter in verteilter Weise dokumentiert. Ein wichtiges Ziel des Projekts war es daher auch, eine systematische Konsolidierung der relevanten Dokumentation im Rahmen eines umfassenden DSFA-Berichts zu erreichen. Dessen Ausarbeitung erfolgte somit in enger Abstimmung mit dem *Verantwortlichen* und hatte mitunter partizipativen bzw „workshop-basierten" Charakter. Festzuhalten ist auch, dass die Leistungen vonseiten des RI als hinzugezogenes Beratungsunternehmen keinesfalls als Audit zu verstehen sind. Das RI ist im Rahmen der DSFA in einer Rolle, die mit einer unabhängigen Auditierung unvereinbar ist. Gleichwohl ist dieser externe Beitrag als wichtiges Instrument der Qualitätssicherung in der Sphäre des *Verantwortlichen* zu sehen. Schließlich wurden im Zuge der Ausarbeitung alle Angaben seitens des *Verantwortlichen* von RI kritisch hinterfragt und die Vorlage der wesentlichen Dokumentation schon aus praktischen Bearbeitungsgründen verlangt. Soweit es in der finalen Entwicklungsphase, auch aus den im Pilotbetrieb gewonnenen Erkenntnissen, noch letzte Lücken in der Umsetzung zu schließen gab, wurde dies mit der kombinierten rechtlichen und technischen Expertise der Berater abgestimmt und mit einer nachvollziehbaren Dokumentation hinterlegt.

Die vorliegend dokumentierte Folgenabschätzung ist wesentlich geprägt durch die laufende technologische Weiterentwicklung des E-ID Systems. Aus methodischer Sicht ist daher schon die Durchführung der DSFA ebenso als dynamischer Prozess zu verstehen, der auf spätere Versionen und

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); https://eur-lex.europa.eu/eli/reg/2016/679/oj.

mögliche Nutzungs- und Einsatzbereiche des E-ID Systems ausgedehnt und entsprechend fortgesetzt werden muss. Dies ist nicht zuletzt auch über Art 35 Abs 11 DSGVO verpflichtend vorgesehen. So ist künftig regelmäßig zu prüfen, ob bzw inwiefern die bisherigen Ergebnisse noch gültig sind und die mit dem E-ID System einhergehenden Datenverarbeitungsprozesse der Risikobeurteilung auch weiterhin standhalten.

In seinem formalen Aufbau geht der vorliegende Bericht in einem ersten Schritt zunächst auf die Frage der rechtlichen Erforderlichkeit einer DSFA ein. Nach dieser sogenannten Schwellwertanalyse folgt die deskriptive Darstellung des Sachverhalts, wobei neben einem allgemeinen Überblick zur technischen Architektur des ID Austria Systems insb auf vier spezifische Datenverarbeitungsprozesse fokussiert wird, nämlich die Registrierung und Akkreditierung der Service Provider, die verschiedenen Varianten der Registrierung der Benutzer*innen, die eigentliche Verwendung der ID Austria sowie schließlich die Verwaltung des E-ID über die Funktion „Meine ID Austria“.

Nach der Beschreibung der wesentlichen tatsächlichen Begebenheiten (Sachverhalt) erfolgt die eigentliche Prüfung der Zulässigkeit der Verarbeitungsvorgänge. Im Zuge dessen werden verschieden datenschutzrechtliche Grundsätze dargestellt und mit Bezug auf das ID Austria System erläutert. Hierzu zählen Aspekte wie die grundsätzliche Frage des Personenbezugs ebenso wie die datenschutzrechtliche Rollenverteilung innerhalb des ID Austria Systems, die Berücksichtigung und Umsetzung der Betroffenenrechte sowie die Analyse der Anforderungen an die Protokollierung.

Auf die normative Analyse folgt die eigentliche datenschutzrechtliche Risikoabschätzung als inhaltlicher Kern und methodisches Herzstück der DSFA. Die Risiken werden pflichtgemäß – dem Schutzzweck des Datenschutzrechts folgend – aus der Perspektive der betroffenen Personen unter Berücksichtigung der Auswirkungen auf die gesamte Gesellschaft erhoben. Dabei befasst sich die Folgenabschätzung insbesondere mit verschiedenen Maßnahmen, Garantien und Verfahren, welche die Risiken der geplanten Verarbeitungsprozesse eindämmen, den Schutz personenbezogener Daten sicherstellen und die Einhaltung der rechtlichen Vorgaben und Bestimmungen nachweisen sollen.[2] Der Bericht mündet schließlich in einer Diskussion der verbleibenden Restrisiken und einer Zusammenfassung der getroffenen Entscheidungen und Ergebnisse der Risikobeurteilung.

[2] Siehe ErwGr 90.

2.1 Erforderlichkeit einer Datenschutz-Folgenabschätzung (Schwellenwertanalyse)

Die Durchführung einer Datenschutz-Folgenabschätzung gem Art 35 DSGVO ist prinzipiell dann erforderlich, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes datenschutzrechtliches Risiko für die Betroffenen besteht.

Nach Art 35 Abs 3 DSGVO ist eine DSFA insbesondere[3] dann erforderlich, wenn eine

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling stützt, und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (gem Art 9 Abs 1 DSGVO)[4] oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten[5] (gem Art 10 DSGVO) durchgeführt wird;
- oder eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche vorgenommen wird.

Darüber hinaus haben die Aufsichtsbehörden eine Liste mit Verarbeitungsvorgängen, für die eine DSFA verpflichtend durchzuführen ist (Blacklist), zu veröffentlichen. Wahlweise können sie zudem eine Liste mit Verarbeitungsvorgängen, für die eine DSFA nicht verpflichtend ist (Whitelist) veröffentlichen.[6] Beides hat die österreichische Datenschutzbehörde getan.[7] Nach der DSFA-AV (Whitelist)[8] ist eine DSFA unter anderem dann nicht notwendig, wenn die Verarbeitung personenbezogener Daten[9] im Rahmen von Registern, die durch Unions-, Bundes-, oder Landesrecht eingerichtet sind, erfolgt.[10] *Trieb* zufolge handelt es sich bei der Whitelist jedoch nicht um Ausnahmen im eigentlichen Sinn, sondern lediglich um eine Klarstellung in Hinblick auf Sachverhalte, die schon den Voraussetzungen der DSGVO für eine DSFA-Pflicht nicht entsprechen.[11]

Dennoch soll zunächst geprüft werden, inwieweit der Ausnahmetatbestand DSFA-A06 (Register, Evidenzen, Bücher) der DSFA-AV relevant sein könnte, also eine Verarbeitung personenbezogener Daten (mit Ausnahme von Daten iSd Art 9 und 10 DSGVO) im Rahmen von durch Unions-, Bundes-, oder Landesrecht eingerichteten Registern vorliegt. Da Datenverarbeitungsvorgänge der ID Austria

[3] Die Aufzählung dieser Regelbeispiele ist also nicht abschließend; *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 36.
[4] Darunter werden nach Art 9 Abs 1 DSGVO personenbezogene Daten verstanden, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person".
[5] Der EuGH hat festgehalten, dass strafrechtliche Daten auch etwa solche über die Erhebung einer Anklage bzw die Berichterstattung bzgl eines Prozesses sein können, auch wenn in diesem keine Straftat festgestellt wird, siehe hierzu: EuGH, C-136/17, ECLI:EU:C:2019:773.
[6] *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 39.
[7] Vgl *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 47, 69; Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) BGBl II 2018/278; Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) BGBl II 2018/108.
[8] Siehe Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV); StF: BGBl. II Nr. 108/2018.
[9] Mit Ausnahme von Daten iSd Art 9 und 10 DSGVO.
[10] DSFA-A06 Anlage 1 DSFA-AV.
[11] *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 47.

zwar unzweifelhaft mit dem Stammzahlenregister bzw dem Ergänzungsregister in einem gewissen Zusammenhang stehen, jedoch wohl nicht ausschließlich *im Rahmen* dieser Register erfolgen, ist dieser Ausnahmetatbestand eher auszuschließen.[12]

Demgegenüber ist eine DSFA nach der sogenannten Blacklist der DSB verpflichtend durchzuführen, wenn unter anderem zumindest **eines** der in § 2 Abs 2 Z 1 – 6 DSFA-V (Blacklist) genannten Kriterien erfüllt ist oder mindestens **zwei** der in § 2 Abs 3 Z 1 – 5 DSFA-V genannten Kriterien erfüllt sind.[13]

Im Zusammenhang mit dem E-ID System könnte insb § 2 Abs 2 Z 4 DSFA-V relevant sein.[14] Demnach ist eine DSFA verpflichtend durch den *Verantwortlichen* durchzuführen, wenn „Verarbeitungen von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen […] erfolgen" wobei exemplarisch auf „den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten" verwiesen wird.

Im Hinblick auf die genannten Kriterien, von denen mindestens **zwei** erfüllt sein müssen, um zu einer DSFA-Pflicht zu führen, erscheint insb Z 2 relevant. Z 2 behandelt die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und deckt sich dabei weitestgehend mit Art 35 Abs 3 lit b zweiter Fall DSGVO (siehe unten). Es ist jedoch anzumerken, dass eine Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen lediglich im Akkreditierungsprozess von privaten Service Providern erfolgt, jedoch nicht im Registrierungsprozess der Benutzer*innen.

Die Artikel-29-Datenschutzgruppe geht weiters davon aus, dass bei Vorliegen von **mindestens zwei** der nachfolgend genannten Kriterien, die Voraussetzungen des Art 35 erfüllt sind und somit eine DSFA erfolgen muss:

1. Bewerten oder Einstufen;
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung;
3. Systematische Überwachung;
4. Verarbeitung von vertraulichen oder höchstpersönlichen Daten;
5. Datenverarbeitung im großen Umfang;

[12] Die entsprechenden Materialien enthalten hierzu keine Spezifizierungen; vgl Erläut DSFA-AV, https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html (abgerufen am 22. 04. 2022); es wird auf Seite 1 jedoch darauf verwiesen, dass an die außer Kraft getretene Standard- und Musterverordnung 2004 (Standard- und Muster-Verordnung 2004 [StMV 2004] BGBl II 2004/312) angeknüpft wird (vgl auch *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 55); diese hatte in ihrer Anlage 1 auf verschiedene öffentliche Register als nicht meldepflichtige Standardanwendungen (§ 1 Abs 1 StMV 2004) Bezug genommen; aus der Beschreibung der Verarbeitungsvorgänge iZm den in der VO genannten Registern kann uE wohl im Allgemeinen geschlossen werden, dass nur unmittelbar mit diesen in Verbindung stehende Verarbeitungsvorgänge gemeint waren: vgl etwa (ua zur Führung des ZPR und Erstellung entsprechender Urkunden) SA008a Anlage 1 StMV 2004; (ua zur Führung des ZSR und zur Ausstellung von Staatsbürgerschaftsnachweisen) SA009a Anlage 1 StMV 2004 sowie (ua zur Führung des ZMR sowie lokalen Melderegisters einschließlich jeweilig zu erstellender Textdokumente wie Korrespondenzen) SA010 Anlage 1 StMV 2004; diese Herangehensweise dürfte sich – trotz der nun mangelnden Beschreibung konkreter Verarbeitungstätigkeiten (vgl *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 56) – mit der DSFA-AV wohl nicht geändert haben (arg „im Rahmen"); zudem erfolgt, wie noch zu erläutern sein wird zT schließlich auch eine Verarbeitung von Daten iSd Art 10 DSG.

[13] Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V); StF: BGBl. II Nr. 278/2018.

[14] In diesem Zusammenhang wäre eben die Erfüllung eines Kriteriums ausreichend.

6. Abgleichen oder Zusammenführen von Datensätzen;
7. Daten zu schutzbedürftigen Betroffenen;
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen;
9. Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw Durchführung eines Vertrags hindert".[15]

Dabei kann im Fall der ID Austria zumindest von einer Datenverarbeitung in großem Umfang gesprochen werden. Die Anwendung kann zudem auch als eine innovative Nutzung neuer technologischer Lösungen gesehen werden. Zudem gilt es zu prüfen, ob bzw inwiefern die Verarbeitung die betroffenen Personen künftig an der Nutzung von Dienstleistungen hindern kann oder Formen systematischer Überwachung beinhaltet bzw ermöglicht.

Darüber hinaus ist in den Leitlinien zur DSFA ausdrücklich festgehalten, dass der *Verantwortliche* auch bei Vorliegen nur **eines** der genannten Kriterien „in einigen Fällen […] von der Notwendigkeit einer DSFA ausgehen muss […]".[16] Was genau unter diese „einigen Fälle" fällt, wird in den Leitlinien zwar nicht weiter thematisiert; es ist jedoch nicht ausgeschlossen, dass eine „Datenverarbeitung im großen Umfang", die potenziell **jede** in Frage kommende[17] Person mit Unions- bzw EWR-Bürgerschaft[18] betreffen kann, wie bei der ID Austria, einen derartigen Fall darstellt.[19] Denn unter Berufung auf ErwGr 91 DSGVO wird als Aspekt dieses Kriteriums etwa „die Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe" genannt.[20] Nachdem der angesprochene Kreis an betroffenen Personen nicht mehr unbedingt nur als Anteil einer Bevölkerungsgruppe bezeichnet werden kann und die konkrete Betroffenenanzahl eine potenziell große ist, liegt hier wohl ein Fall dieses in den Leitlinien definierten Kriteriums vor. Darüber hinaus sind die Folgen des Einsatzes der ID Austria sowohl für einzelne Betroffene als auch für die gesamte Gesellschaft aufgrund des potenziell großen Anwendungsbereichs (noch) schwer abzuschätzen.

Dem neunten Fall der Leitlinien entspricht ein Verarbeitungsvorgang unter anderem dann, wenn er betroffene Personen **an der Ausübung einer Dienstleistung oder Durchführung eines Vertrags hindert**. Die Art 29 Datenschutzgruppe verweist dabei auf Art 22 und ErwGr 91 DSGVO zur automatisierten Einzelentscheidung und nennt als Beispiel eine Bank, die Daten von Kreditauskunfteien verarbeitet, um Entscheidungen über Kreditvergaben zu treffen.[21] Diesbezüglich gilt es klarzustellen, dass das ID Austria System an sich keine automatisierte Einzelentscheidung

[15] *Artikel-29-Datenschutzgruppe,* Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", (17/DE WP 248 Rev. 01) 13.
[16] *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 13.
[17] Dies nämlich selbstverständlich mit der Einschränkung, dass diese die entsprechenden Voraussetzungen erfüllen.
[18] Denn die in den Mitgliedstaaten der EU unmittelbar anwendbare eIDAS-VO wurde grundsätzlich auch in das EWR-Abkommen übernommen; vgl Beschluss des Gemeinsamen EWR-Ausschusses 22/2018 vom 9. 2. 2018 zur Änderung von Anhang XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) des EWR-Abkommens [2019/2058], ABl L 323/2019, 45.
[19] Vgl auch *Trieb,* wonach der „Umfang" etwa anhand der Zahl der betroffenen Personen (etwa auf regionaler Ebene) bewertet werden kann: *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 33 (Stand 1. 9. 2019, rdb.at).
[20] *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 11.
[21] Siehe *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 12 f.

impliziert, wie dies bspw im Fall von Credit Scoring Prozessen der Fall ist.[22] Vielmehr soll das ID Austria System die Nutzung bzw den Zugang zu diversen Anwendungen und Services ermöglichen und grundsätzlich erleichtern.

Außerdem ist zumindest im Hinblick auf den Verarbeitungsvorgang „Registrierung und Akkreditierung von privaten Service Providern“ festzuhalten, dass – wie im Folgenden noch gezeigt wird – eine umfangreiche Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten gem Artikel 10 DSGVO vorliegt. Die Verarbeitung kann deswegen als umfangreich angesehen werden, weil der Kreis der Personen, die sich um eine Akkreditierung ihres Service Providers bewerben könnten, potenziell sehr groß ist, da es sich um ein mehr oder weniger[23] allgemein zugängliches, von staatlicher Seite zur Verfügung gestelltes System handeln soll bzw jeder interessierte Service Owner dies in Anspruch nehmen könnte. Im Hinblick auf Art 35 Abs 3 lit b zweiter Fall DSGVO wird somit wohl auch dieser Aspekt die Durchführung einer DSFA erforderlich machen.[24]

Zudem ist zu prüfen, ob die Datenverarbeitung unter Nutzung neuartiger organisatorischer oder technischer Lösungen erfolgt, die die Abschätzung der Auswirkungen auf betroffene Personen und gesellschaftliche Folgen erschweren.[25] Dieser Tatbestand der DSFA-V entspricht im Wesentlichen dem achten Kriterium der Art-29-Datenschutzgruppe[26], dementsprechend soll im Folgenden, sofern sinnvoll, vor allem dieses behandelt werden. Dabei fällt auf, dass die in diesem Zusammenhang in den Leitlinien vorgebrachten Beispiele[27] eher neuartige **technische** Komponenten enthalten.[28] Diesen Überlegungen dürfte der Gedanke zugrunde gelegen sein, dass vor allem die Verwendung von neuartiger Technologie[29] tendenziell unvorhersehbare Folgen haben kann.

Im Hinblick auf die ID Austria ist daher fraglich, ob auf kryptografischen Verfahren beruhende Datenverarbeitungen, die im Wesentlichen auch auf den vieljährigen Erfahrungen mit Systemen wie der Handy-Signatur aufbauen, derartige Neuartigkeit innehaben.

---

[22] Siehe hierzu weiterführend *Rothmann/Sterbik-Lamina/Peissl*, Credit Scoring in Österreich (2014).

[23] Derzeit ist dies nur für Unternehmer und Vereine möglich, aufgrund einer entsprechenden Ermächtigung im Gesetz ist aber vorgesehen, dass durch Verordnung eine Ausdehnung auf andere Personen (zu denken wäre auch an „Privatpersonen“) erfolgen kann; vgl § 18 Abs 3 E-GovG.

[24] Darüber hinaus ist bzgl dieser Datenkategorien der vierte Fall der Leitlinien des EDSA gegeben: siehe *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 11.

[25] Also ob § 2 Abs 2 Z 4 DSFA-V erfüllt ist; Die Materialien enthalten keine Spezifikationen darüber, was eine neuartige organisatorische Lösung darstellen könnte; siehe Erläut DSFA-V, https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html (abgerufen am 22. 04. 2022).

[26] Siehe *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 72.

[27] Vgl *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 12 f; fast wortgleich im Übrigen auch Erläut DSFA-V, https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html (abgerufen am 22. 04. 2022).

[28] So wird auf (wenngleich wohl zugleich organisatorische) Lösungen eingegangen, die jeweils Erkennungstechnologien – vermutlich meist unter Einsatz von künstlicher Intelligenz – verwenden: siehe zur Kombination von Fingerabdruck- und Gesichtserkennung zur Zugangskontrolle: *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 12; siehe zur automatischen Kennzeichenerfassung im Rahmen eines Schnellstraßenüberwachungssystems: *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 13; dies erfolgt mit einem Hinweis auf ErwGr 91 der DSGVO, wonach eine neue Technologie eine solche ist, *die dem jeweils aktuellen Stand der Technik entspricht*. Als Argument wird diesfalls vorgebracht, dass dabei neuartige Formen der Datenerfassung und -nutzung vonstattengehen könnten, die ein hohes Risiko bergen, so etwa IoT-Anwendungen aufgrund deren Auswirkung auf Alltag und Privatleben von betroffenen Personen (vgl *Artikel-29-Datenschutzgruppe,* Leitlinien [17/DE WP 248 Rev. 01] 12.).

[29] Wenngleich im Rahmen altbekannter Problemlösungen: so etwa Videoüberwachungssysteme auf Schnellstraßen: vgl erneut *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 13.

Die Leitlinien[30] führen aber im Rahmen dieses Kriteriums auch die **innovative Nutzung** an. Dazu ist zu sagen, dass die Bereitstellung bzw Übermittlung von (zusätzlichen) Attributen iSv Personenmerkmalen auf Basis staatlicher Register ein relativ neues Phänomen darstellt. Dieses beruht zwar auch auf dem Gedanken der Datenminimierung,[31] dennoch wird diese Art der Datenübermittlung wohl erst seit Kürzerem genutzt.[32] Man könnte demnach ableiten, dass solche Systeme nach dem aktuellen Stand der Technik eine **innovative Nutzung** darstellen. Dies würde sich auch mit dem Kriteriums decken, wonach mit entsprechenden Verarbeitungsvorgängen möglicherweise ein hohes Risiko einhergehen kann. Denn bei einem neuartigen Einsatz (wenngleich „alter" Methoden, wie kryptografischer Verfahren etc) könnte man ein Risiko darin sehen, dass Nutzer*innen mit der Funktionsweise der Systeme nicht vertraut sind und zunächst unter Umständen nicht verstehen, wie und welche Daten dabei verarbeitet werden.[33] Auch im Hinblick darauf, dass bei der ID Austria Biometrie-Erkennungssysteme (wenngleich ausschließlich auf den Geräten der jeweiligen Benutzer*innen) zusammen mit verschiedenen anderen Komponenten[34] in einem komplexen Gesamtsystem[35] zur Anwendung kommen und dieses System das Potenzial hat, sich erheblich auf den Alltag und das Privatleben von Personen auszuwirken[36], ist die Anwendbarkeit dieses Kriteriums durchaus wahrscheinlich.[37] Dabei könnten nicht zuletzt auch die wie erwähnt schwierig abzuschätzenden Folgen des Einsatzes der ID Austria für Einzelne, wie auch für die Gesellschaft als Ganzes wegen des potenziell sehr großen Anwendungsbereichs und der vermutlich stetig steigenden Nutzer*innenzahl, eine Rolle spielen.

Zu prüfen ist weiters, inwiefern im Zusammenhang mit dem ID Austria System von einer **systematischen Überwachung** gesprochen werden kann. Dies hängt zunächst von der Definition des Begriffs „Überwachung" ab; der kanadische Soziologe David Lyon geht bspw von einem weiten Verständnis aus und definiert Überwachung (Surveillance) als „any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered".[38] Zudem zeigen politikwissenschaftliche Studien, dass ID Systeme in der (europäischen) Vergangenheit wiederholt zu staatlichen Überwachungs- und Kontrollzwecken genutzt

[30] Siehe *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 12.
[31] So wäre etwa nicht mehr die Speicherung des gesamten Ausweisdokuments notwendig, sondern zB nur die Übermittlung des Geburtsdatums zur Alterskontrolle, was ja durchaus eine datenschutzfreundliche Eigenschaft darstellt.
[32] Vgl hierzu auch die Begründung des Vorschlags der EU-Kommission zur Anpassung der eIDAS-VO, wonach sich iZm elektronischen Identitäten „auf dem Markt [...] ein **neues** Umfeld [abzeichnet], in dem sich der Schwerpunkt [...] auf die Bereitstellung und Verwendung einzelner Attribute [...] verlagert hat": proposal for a regulation of the European Parliament and of the Council amending regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM (2021) 281 final 2021/0136 (COD), 1.
[33] Das Vorweisen eines Führerscheins zur Alterskontrolle ist für eine technisch nicht versierte Nutzer*in wohl unstrittig transparenter als die (unter 3.2.3.3. näher erläuterte) Anmeldung bzw (zusätzliche) Attributsübermittlung aus einem komplexen System wie der ID Austria (wenngleich sich diese uU als datensparsamer erweist).
[34] Sowohl technischer als auch organisatorischer Natur, wobei der derart umfassende Anwendungsbereich des Systems wohl durchaus als neuartig bezeichnet werden kann; siehe zur Verwendung biometrischer Identifikationsmethoden insbesondere 3.2.3; siehe zu den Komponenten im Detail 3.2.2.1.
[35] Arg: zumindest komplexe, wenngleich nicht unbedingt gänzlich neuartige technische bzw organisatorische Lösungen, gleichzeitig wohl durchaus innovative Nutzung; siehe zum Gesamtsystem insbesondere 3.2.2.1.
[36] Vgl erneut *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 12.
[37] Für den entsprechenden Tatbestand der "Blacklist" könnte demnach ähnliches gelten.
[38] *Lyon*, Surveillance society (2001) 2.

bzw entfremdet wurden.[39]Nach der deutschen Sprachfassung der Artikel-29-Datenschutzgruppe Leitlinie müsste es sich für die Begründung einer DSFA um Verarbeitungstätigkeiten handeln, „die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum **Ziel haben** und auf beispielsweise über Netzwerke erfasste Daten […] zurückgreifen".[40] Unter „systematisch" versteht die Artikel-29-Datenschutzgruppe unter anderem „im Rahmen eines Systems stattfindend".[41] Die systematische Komponente könnte – allgemein und abstrakt betrachtet – bei einem komplexen Gesamtsystem wie der ID Austria durchaus gegeben sein.[42] Jedoch haben die dabei erfolgenden Verarbeitungsvorgänge die Überwachung oder Kontrolle der Nutzer*innen als Betroffene gerade **nicht zum Ziel**. Ganz im Gegenteil sollen Nutzer*innen das ID Austria System möglichst unbeobachtet nutzen können, was etwa dadurch zum Ausdruck kommt, dass Protokolldaten der Datenübermittlung aus dem System gem § 18 Abs 1 letzter Satz E-GovG grundsätzlich nur dem *E-ID-Inhaber* selbst zugänglich sein sollen. Die englische Sprachfassung der Leitlinien spricht zwar eher von der Nutzung („used to") der Verarbeitung zu den genannten Überwachungszwecken[43], jedoch ist beides im Hinblick auf Nutzer*innen eher anzuzweifeln, da diese potenzielle Abweichung wohl nicht beabsichtigt ist und vermutlich weniger auf die schlichte Möglichkeit der entsprechenden Verwendung (bzw des Missbrauchs) der Daten, sondern eher auf die tatsächlich vorgesehenen bzw geplanten **Verarbeitungsvorgänge im Rahmen des Systems** abzustellen sein wird.[44] Davon abgesehen könnte aber zumindest im Hinblick auf die Überprüfung von privaten Service Providern bzw Service Ownern eine entsprechende „Kontrolle" vorliegen.

Abschließend ist noch zu prüfen, inwieweit der Ausnahmetatbestand DSFA-A06 (Register, Evidenzen, Bücher) der DSFA-AV relevant sein könnte, also eine Verarbeitung personenbezogener Daten (mit Ausnahme von Daten iSd Art 9 und 10 DSGVO) im Rahmen von durch Unions-, Bundes-, oder Landesrecht eingerichteten Registern vorliegt. Da Datenverarbeitungsvorgänge der ID Austria zwar unzweifelhaft mit dem Stammzahlenregister bzw dem Ergänzungsregister in einem gewissen Zusammenhang stehen, jedoch wohl nicht ausschließlich *im Rahmen* dieser Register erfolgen, ist dieser Ausnahmetatbestand auszuschließen.[45]

---

[39] Siehe hierzu die Ausführungen in *Boersma/Van Brakel/Fonio/Wagenaar*, Histories of State Surveillance in Europe and Beyond (2014) 133 ff über „ID-Cards as a surveillance method to govern societies" mit Fallbeispielen zu Spanien, den Niederlanden, Belgien oder Großbritannien.

[40] *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) 10.

[41] *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) FN 15; vgl in der englischen Sprachfassung: „occuring according to a system", *Artikel-29-Datenschutzgruppe,* Leitlinien (17/EN WP 248 Rev. 01) FN 15.

[42] Siehe hierzu noch sogleich.

[43] Dies stellt uE eine gewisse Abweichung dar, zumal zumindest das geplante **Ziel** eines Verarbeitungsprozesses und wozu dieser (tatsächlich) **genutzt** wird, divergieren könnte.

[44] Vgl zur Definition von „systematisch" erneut *Artikel-29-Datenschutzgruppe,* Leitlinien (17/DE WP 248 Rev. 01) FN 15.

[45] Die entsprechenden Materialien enthalten hierzu keine Spezifizierungen; vgl Erläut DSFA-AV, https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html (abgerufen am 22. 04. 2022), es wird auf Seite 1 jedoch darauf verwiesen, dass an die außer Kraft getretene Standard- und Musterverordnung 2004 (Standard- und Muster-Verordnung 2004 [StMV 2004] BGBl II 2004/312) angeknüpft wird; vgl auch *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 55; diese hatte in ihrer Anlage 1 auf verschiedene öffentliche Register als nicht meldepflichtige Standardanwendungen (§ 1 Abs 1 StMV 2004) Bezug genommen; aus der Beschreibung der Verarbeitungsvorgänge iZm den in der VO genannten Registern kann uE wohl im Allgemeinen geschlossen werden, dass nur unmittelbar mit diesen in Verbindung stehende Verarbeitungsvorgänge erfasst waren: vgl etwa (ua zur Führung des ZPR und Erstellung entsprechender Urkunden) SA008a Anlage 1 StMV 2004; (ua zur Führung des ZSR und zur Ausstellung von Staatsbürgerschaftsnachweisen) SA009a Anlage 1 StMV 2004 sowie (ua zur Führung des ZMR sowie lokalen Melderegisters einschließlich jeweilig zu erstellender Textdokumente wie Korrespondenzen) SA010 Anlage 1 StMV 2004; diese

Auf Basis der vorangegangenen Ausführungen kann somit festgehalten werden, dass die Implementierung des ID Austria Systems die Durchführung einer DSFA aus einer Reihe von Gründen erforderlich macht. Dabei kann insb auf den großen Umfang der geplanten Datenverarbeitung verwiesen werden. Darüber hinaus kommt es – wenngleich ausschließlich am Gerät der jeweiligen Benutzer*innen – zu einem Einsatz biometriebasierter Authentifizierungsmethoden, sowie das System an sich als neuartiger organisatorischer bzw technischer Datenverarbeitungskomplex verstanden werden kann, der die Abschätzung der Auswirkungen und Folgen auf und durch betroffene Personen erschwert.

Nicht zuletzt ist zudem darauf hinzuweisen, dass in den Materialien zum E-Government-Gesetz[46] festgehalten wurde, dass „intensive Arbeiten an einer Informationssicherheits- und Datenschutzrisikoanalyse des E-ID Systems“ laufen und eine den Vorgaben der DSGVO entsprechende Datenschutz-Folgenabschätzung in Aussicht genommen wird, die zeitgerecht vor Inbetriebnahme vorliegen soll. Dabei soll die DSFA insb „hinsichtlich der Verwendung von besonders schützenswerten Daten iSd Art 9 DSGVO durchgeführt werden.“ Die Durchführung einer systematischen Abschätzung der (datenschutzrechtlichen) Folgen des ID Austria Systems ist somit erforderlich.

Herangehensweise dürfte sich – trotz der nun mangelnden Beschreibung konkreter Verarbeitungstätigkeiten – mit der DSFA-AV wohl nicht geändert haben (arg „im Rahmen“); vgl *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 56.

[46] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG); StF: BGBl. I Nr. 10/2004.

3 Sachverhaltsdarstellung und Spezifizierung des Prüfgegenstands

Mit der Novellierung des E-Government-Gesetzes[47] 2017 kommt es zu einer Weiterentwicklung von Bürgerkarte bzw Handy-Signatur zur sogenannten ID Austria. Die ID Austria ist die österreichische Variante des elektronischen Identitätsnachweises (E-ID) zur eindeutigen Identifikation der Bürger*innen gegenüber digitalen Anwendungen und Diensten sowohl aus dem behördlichen als auch privaten Umfeld.[48]

Diese über die eIDAS-VO[49] forcierte Implementierung einer elektronischen Identität soll die persönliche Authentifizierung im Internet erleichtern sowie Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel beseitigen.[50] Durch den E-ID soll es Bürger*innen möglich sein, sich online auszuweisen, digitale Services zu nutzen und Geschäfte rechtsverbindlich auf elektronischem Wege abzuschließen.

Dabei werden die bisher bekannten Nutzungsmöglichkeiten von Handy-Signatur und Bürgerkarte mit Einführung der ID Austria erweitert, sodass künftig neben dem Minimaldatensatz (MDS) bestehend aus Vor-, Nachname und Geburtsdatum auch weitere Personenmerkmale (Attribute) wie zB Führerschein- und Meldedaten verarbeitet werden können.[51] Die ID Austria soll zudem ermöglichen, dass auch rein App-basierte Provider mobiler Services den elektronischen Identitätsnachweis nutzen können.[52]

Das ID Austria System wird über die App „Digitales Amt“[53] sowie über die Website „oesterreich.gv.at“[54] angeboten. Die App ist (kostenlos) via Download über den Play Store[55] von Google sowie den App Store von Apple[56] erhältlich. Seit Jänner 2021 befindet sich die ID Austria in einer Pilotphase. Noch im Verlauf des Jahres 2022 soll die ID Austria allen Bürger*innen in vollem Umfang zur Verfügung stehen.

Inhalt des vorliegenden Berichts ist die nach Art 35 Abs 1 DSGVO erforderliche Abschätzung datenschutzrechtlicher Folgen der im Rahmen der ID Austria vorgesehenen Verarbeitungsvorgänge. Damit verbunden ist die Betrachtung der durch das System ausgelösten (personenbezogenen) Datenflüsse ebenso wie die sicherheitstechnische Ausgestaltung und Architektur des Systems, inklusive der dabei getroffenen technischen und organisatorischen Maßnahmen der Risikomitigierung.

---

[47] E-Government-Gesetz BGBl I 2004/10 idF BGBl I 2017/121.
[48] Ein elektronischer Identitätsnachweis ist gem § 2 Z 10 E-GovG definiert als eine logische Einheit, die eine qualifizierte elektronische Signatur mit einer Personenbindung und den zugehörigen Sicherheitsdaten und -funktionen verbindet.
[49] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.
[50] Vgl ErwGr 12 eIDAS-VO.
[51] Vgl ErläutRV 469 BlgNR 27. GP 2. Gemäß § 4 Abs 1 E-GovG dient der E-ID „[...] dem Nachweis der eindeutigen Identität, weiterer Merkmale sowie des Bestehens einer Einzelvertretungsbefugnis eines *Einschreiters* und der Authentizität des elektronisch gestellten Anbringens in Verfahren, für die ein Verantwortlicher des öffentlichen Bereichs eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet hat.“
[52] Trotz ihres mobilen Charakters war die Handy-Signatur bisher auf eine Verwendung über klassische Endnutzergeräte wie PCs oder Laptops beschränkt. Das mobile Gerät (Handy, Smartphone) kam dabei nur als Zweitgerät im Zuge der Benutzerauthentifizierung zum Einsatz.
[53] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/faq/app_digitales_amt.html (abgerufen am 22. 04. 2022).
[54] Siehe https://www.oesterreich.gv.at/id-austria.html (abgerufen am 22. 04. 2022).
[55] Siehe https://play.google.com/store/apps/details?id=at.gv.oe.app&hl=de_AT&gl=US (abgerufen am 22. 04. 2022).
[56] Siehe https://apps.apple.com/at/app/digitales-amt/id1454775189 (abgerufen am 22. 04. 2022).

Im Fokus stehen dabei die vier nachfolgend angeführten Verarbeitungstätigkeiten:

- Registrierung und Akkreditierung behördlicher und privater Service Provider;[57]
- Registrierung der Benutzer*innen (ID-Werber*in wird zu *ID-Inhaber*);[58]
- Verwendung der ID Austria;[59]
- Verwaltung der ID Austria durch die Benutzer*innen (über die Funktion „Meine ID Austria“ in der App „Digitales Amt“ bzw via Weboberfläche).[60]

Die vorliegende DSFA beschränkt sich auf die Analyse der hier angeführten Verarbeitungstätigkeiten des ID Austria Systems. Dabei liegt der Fokus der Diskussion wiederum insb auf der Klärung der datenschutzrechtlichen Rollenaufteilung (*Verantwortliche/Auftragsverarbeiter*) sowie der Aufzeichnung, Einsicht und Aufbewahrung von Transaktions-Logs und Einwilligungserklärungen. Die Datenschutz-Folgenabschätzung gipfelt in einer Beschreibung der Risikoszenarien für die Rechte und Freiheiten der betroffenen Personen und der Bewertung dieser Risiken anhand einer Risikomatrix.

Datenverarbeitungen, die zwar aus praktischer Sicht im Zuge der Verwendung der ID Austria erfolgen, jedoch in formalrechtlicher Hinsicht nicht mehr dem ID Austria System zuzurechnen sind, sind auch nicht Teil der vorliegenden DSFA. Dies bezieht sich insb auf künftige Dienste und Anwendungen privater Service-Provider. Darüber hinaus erfolgt eine Abgrenzung gegenüber Anwendungen wie dem sog Portalverbund[61] sowie dem Unternehmensserviceportal (USP),[62] welche als Schnittstelle behördlicher und privater Service Provider der Registrierung über das Service Provider-Register-Service des ID Austria Systems dienen bzw dieser vorangestellt sind.[63] Weiters erfolgt eine Abgrenzung gegenüber den AGB, der Datenschutzerklärung sowie dem Signaturvertrag des *Vertrauensdiensteanbieters* (VDA) A-Trust.

Die vorliegende DSFA erstreckt sich zudem lediglich auf jene Bereiche der App „Digitales Amt“, die in unmittelbarem Zusammenhang mit der Verwendung der ID Austria stehen. Diese Abgrenzung ist insofern relevant, da die App grundsätzlich über einen breiten Funktionsumfang verfügt und als zentraler Einstiegspunkt in diverse mobile E-Government-Services dient. Dazu zählen auch Funktionen wie zB der sog Digitale Babypoint oder die Online-Beantragung einer Wahlkarte. Soweit aus datenschutzrechtlicher Sicht erforderlich werden angrenzende Dienste und Funktionen in der Folgenabschätzung berücksichtigt und in die Analyse miteinbezogen.

Im Folgenden wird der Sachverhalt anhand der Architektur des ID Austria Systems sowie der einzelnen Datenverarbeitungsprozesse von Registrierung über Nutzung bis hin zur Verwaltung aufgeschlüsselt und erläutert.

[57] Siehe dazu im Detail 3.2.1.
[58] Siehe dazu im Detail 3.2.2.
[59] Siehe dazu im Detail 3.2.3.
[60] Siehe dazu im Detail 3.2.4.
[61] Siehe https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).
[62] Siehe https://www.usp.gv.at/ (abgerufen am 22. 04. 2022).
[63] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner (2021) 19.

3.1 Technische Architektur der ID Austria

Die Architektur des ID Austria Systems setzt sich aus verschiedenen Teilbereichen (Domains) zusammen. Jede Domain enthält eine oder mehrere (technische) Komponenten, die wiederum von einer Organisation (wie zB dem BRZ oder dem BMI) betrieben werden und eine bestimmte Funktion des Systems erfüllen sollen.[64] Nachfolgende Abbildung zeigt die Domains des ID Austria Systems sowie relevante Schnittstellen zwischen den verschiedenen Bereichen.

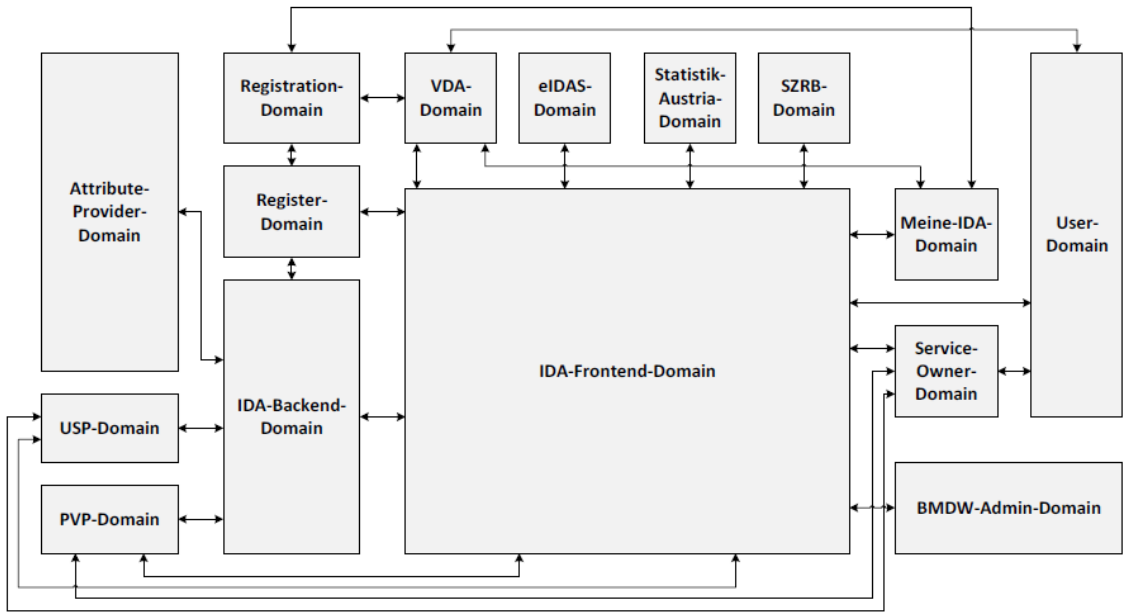

Abbildung 1: Architektur der ID Austria - Domain Ebene mit wesentlichen Schnittstellen.

Das funktionale Zusammenwirken der verschiedenen Bereiche und Komponenten des ID Austria Systems lässt sich wie folgt zusammenfassen:[65]

Für die Verwendung des E-ID ist es zunächst erforderlich, dass sich die Benutzer*innen persönlich im System registrieren. Dies erfolgt über definierte, organisatorische Prozesse und technische Komponenten, die in der Registration-Domain angesiedelt sind. Die Registration-Domain und ihre Komponenten werden vom BMI bereitgestellt.

Die Registration-Domain verfügt über eine Schnittstelle zur User-Domain (also den Komponenten rund um den *E-ID-Inhaber*), da die Benutzer*innen mit ihren Endgeräten mit Komponenten der Registration-Domain interagieren müssen.

Die Registration-Domain verfügt zudem über weitere Schnittstellen zur Backend-Domain und zur VDA-Domain. Erstere ist ebenfalls im Bereich des BMI angesiedelt und beinhaltet unter anderem das für die Registrierung einer persönlichen ID Austria notwendige Stammzahlenregister (SZR).

[64] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 11 ff.
[65] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 11 ff.

Die VDA-Domain repräsentiert hingegen den Bereich des *Vertrauensdienstanbieters* (VDA), der im Zuge der Registrierung einer ID Austria ein qualifiziertes Signaturzertifikat für Benutzer*innen ausstellt.

Nach erfolgter Registrierung können die Benutzer*innen ihre ID Austria in Verbindung mit verschiedenen Services und Anwendungen verwenden. Die Anbieter*innen derartiger Services und Anwendungen sind in der Service Owner-Domain angesiedelt.

Die Service Owner-Domain verfügt über eine Schnittstelle zur User-Domain, über welche Benutzer*innen bereitgestellte Dienste des Service Providers in Anspruch nehmen können. Der jeweilige Service Provider nutzt die ID Austria seinerseits zur gesicherten Anmeldung bzw Authentifizierung der Benutzer*innen. Dementsprechend verfügt die Service Owner-Domain auch über eine Schnittstelle zur Frontend-Domain. Diese wird durch das Bundesrechenzentrum (BRZ) betrieben und stellt unter anderem jene Schnittstellen bereit, über die Service Provider Anmeldeprozesse initiieren können.

Um das ID Austria System nutzen zu können, müssen sich (private) Service Provider zunächst aber selbst registrieren und akkreditieren lassen. Dies erfolgt unter anderem über Komponenten in der Unternehmensserviceportal/Portalverbundprotokoll-Domain (USP/PVP-Domain), weshalb auch hier eine Schnittstelle zwischen der Service Provider-Domain und der USP/PVP-Domain existiert.

Als Kernaufgabe der Frontend-Domain gilt wiederum die Authentifizierung der Benutzer*innen. Diese erfolgt im Falle der Verwendung eines bereits registrierten E-ID über den *Vertrauensdienstanbieter* (VDA), der in der VDA-Domain angesiedelt ist. Dementsprechend verfügt die Frontend-Domain über eine Schnittstelle zur VDA-Domain.

Für Bürger*innen anderer EU-Mitgliedsstaaten kann eine Authentifizierung auch über den eIDAS-Framework erfolgen. Komponenten des eIDAS-Frameworks sind der eIDAS-Domain zugeordnet, die sich ebenfalls im Hoheitsgebiet des BMI befindet, und über eine Schnittstelle zur Frontend-Domain verfügt. Sowohl VDA-Domain als auch eIDAS-Domain haben eine Schnittstelle zur User-Domain, über welche die Benutzer*innen authentifiziert werden. Auch die Frontend-Domain selbst verfügt über eine Schnittstelle zur User-Domain, da auch hier zur Authentifizierung eine Interaktion mit den Benutzer*innen notwendig ist.

Da sich die Benutzer*innen auch mittels Vollmacht in Vertretung für andere Personen anmelden können, benötigt die Frontend-Domain zudem eine Anbindung an Komponenten, die relevante Vollmachten-Informationen bereitstellen. Solche Komponenten sind in der Statistik-Austria-Domain, der Stammzahlenregisterbehörden-Domain (SZRB-Domain) und der USP/PVP-Domain angesiedelt.[66]

In der folgenden Liste werden die einzelnen Bereiche des Systems aufgeschlüsselt und kurz erläutert:

User-Domain

Die User-Domain bezeichnet die Umgebung des *E-ID-Inhabers*, von der aus dieser die ID Austria verwendet. Dementsprechend umfasst die User-Domain den *E-ID-Inhaber* selbst (als Nutzer*in) sowie

[66] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 11 ff.

dessen Geräte (wie zB das Mobiltelefon oder ein anderes internetfähiges Endgerät). Über Komponenten innerhalb der User-Domain erfolgt die Interaktion mit dem VDA zur Authentifizierung des *E-ID-Inhabers*. Für die Abwicklung des Anmeldeprozesses existiert zudem eine Schnittstelle zur IDA-Frontend-Domain.

Service Owner-Domain

Dieser Bereich enthält im Wesentlichen den bereitgestellten Dienst bzw die Applikation, die das ID Austria System eingebunden hat und zum Zweck der Authentifizierung der Benutzer*innen einsetzt. Die Service Owner-Domain repräsentiert daher die Anwendung einer bestimmten Organisation (Service Owner) und deren Schnittstelle zum ID Austria System.[67] Die Benutzer*innen lösen in dieser Anwendung den Anmeldeprozess über das E-ID System aus. Der Begriff „Service Provider" bezeichnet ein technisches Service, das Endnutzer*innen angeboten wird. Der Begriff „Service Owner" bezeichnet die für den Service Provider verantwortliche Organisation. Dies kann eine Organisation des öffentlichen Sektors (zB ein Ministerium) oder auch ein privatwirtschaftliches Unternehmen sein. Ein Service Owner kann dabei für eine beliebige Anzahl an Service Providern verantwortlich sein.

Meine-IDA-Domain

Diese Domain enthält die Applikation und Website „Meine ID Austria" inkl dem Vorregistrierungssystem. Dabei handelt es sich um eine Anwendung, über die der *E-ID-Inhaber* seinen E-ID verwalten kann. Dazu gehören die Einsicht in Transaktions-Logdaten[68], das Auslösen von Widerrufsprozessen[69] oder auch die partielle Durchführung von Registrierungsschritten[70].

E-ID-Frontend-Domain

Die E-ID-Frontend-Domain implementiert notwendige Funktionalitäten zur Authentifizierung von Benutzer*innen im Zuge von Anmeldeprozessen an Services und Applikationen[71], die über eine Anbindung zum ID Austria System verfügen. Die verschiedenen Funktionalitäten werden durch verschiedene technische Komponenten wie zB den Shibboleth Indentity Provider (IDP)[72] zur Authentifizierung des E-ID-Inhabers und die Aggregation aller notwendigen Identitätsattribute oder das Binding Service[73] zur vereinfachten wiederholten Authentifizierung realisiert. Die E-ID-Frontend-Domain beinhaltet auch das „ZLog". Hierbei handelt es sich um das zentrale Logging-System der E-ID-Frontend-Domain, welches Transaktionen dokumentiert.

[67] Dies könnte etwa eine Webapplikation sein, welcher über die Einbindung der ID Austria eine gesicherte Anmeldung von Nutzer*innen ermöglicht.
[68] Hierdurch soll den Benutzer*innen ermöglicht werden, nachzuvollziehen, welche Transaktionen mit der jeweiligen ID Austria getätigt wurden.
[69] Hierbei kann etwa das qualifizierte Zertifikat durch den *E-ID-Inhaber* beim VDA widerrufen werden.
[70] Siehe zu diesen insbesondere 3.2.2.
[71] Siehe zu diesen insbesondere 3.2.3.
[72] Shibboleth ist ein Verfahren zur verteilten Authentifizierung und Autorisierung für Webanwendungen und Webservices.
[73] Siehe hierzu Kapitel 3.2.3.2.

IDA-Backend-Domain

Die IDA-Backend-Domain beinhaltet hauptsächlich Funktionalitäten zur Zusammenführung von Attributen[74] im Zuge von Anmeldeprozessen an Services und Applikationen. Hierzu zählen bspw der Attribute-Handler mit Zugriff auf das Stammzahlenregister sowie die Komponenten der Service Provider-Akkreditierung.

Attribute Provider-Domain

Die Attribute Provider-Domain implementiert die notwendige Funktionalität zur Bereitstellung von Attributen im Zuge von Anmeldeprozessen an Applikationen. Diese Funktionalität wird hierbei durch diverse technische Komponenten umgesetzt. Im Wesentlichen handelt es sich dabei um verschiedene öffentliche und private Register.[75]

Registration-Domain

Die Registration-Domain enthält jene Entitäten, die für die Durchführung der Registrierung des E-ID eines (zukünftigen) *E-ID-Inhabers* notwendig sind. Entsprechend den definierten Registrierungsprozessen[76] sind sowohl technische Komponenten als auch (natürliche) Personen Entitäten dieser Domain. Als nicht-technische Komponente fungieren in der Registration-Domain jene Mitarbeiter*innen der Passbehörde, die den Registrierungsprozess behördenseitig durchführen. Unterstützt werden die Mitarbeiter*innen dabei von der Komponente Identitätsdokumentenregister (IDR), die ebenfalls in der Registration-Domain angesiedelt ist. Das Identitätsdokumentenregister (IDR) beinhaltet Daten zur Person, wie zB Reisepässe, Personalausweise, die zur sicheren Identifikation benötigt werden. Bei der Registrierung eines E-ID wird das Identitätsdokumentenregister vom *Vertrauensdienstanbieter* (VDA) zur Abfrage von Personendaten benötigt. Ebenso verwendet das Stammzahlenregister (SZR) das IDR zur Prüfung, ob ein E-ID aktiviert und gültig ist. Im Zuge der Registrierung eines neuen E-ID bietet das IDR den Mitarbeiter*innen der Passbehörde das dafür notwendige User-Interface an. Über dieses können die Mitarbeiter*innen den Teil der Registrierung, der in der Behörde durchzuführen ist, gemeinsam mit dem zukünftigen *E-ID-Inhaber* abwickeln.

VDA-Domain

Die VDA-Domain beinhaltet den *Vertrauensdienstanbieter* (VDA). Der VDA stellt die Infrastruktur für die Authentifizierung von Benutzer*innen mittels qualifizierter elektronischer Signaturen bereit. Aktuell wird die Rolle des VDA von der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH wahrgenommen. Die Erstellung der qualifizierten Signatur durch den *E-ID-Inhaber* stellt sowohl die Authentifizierung des *E-ID-Inhabers* als auch die Einverständniserklärung zur Freigabe der Attribute durch den *E-ID-Inhaber* dar.

[74] Attribute sind in diesem Zusammenhang als Information bzw Variable wie zB das Vorhandensein einer Lenkberechtigung zu verstehen.
[75] Relevante Register wären in diesen Zusammenhang bspw ZMR, ZPR und FSR.
[76] Siehe zu diesen insbesondere 3.2.2.

eIDAS-Domain

Alternativ zur VDA-Domain kann die Authentifizierung des *E-ID-Inhabers* im Zuge eines Anmeldeprozesses an einer Applikation auch über die eIDAS-Domain erfolgen. Die eIDAS-Domain enthält mit dem österreichischen eIDAS-Knoten (eIDAS-Knoten AT) nur eine einzige Komponente. Der österreichische eIDAS-Knoten stellt jedoch die Schnittstelle in das europäische eIDAS-Netzwerk dar, welches für die Identifikation und Authentifizierung von *Inhabern* ausländischer E-IDs verwendet werden kann.

Statistik-Austria-Domain (SAD)

Diese Domain ist ausschließlich bei einer Anmeldung an Applikationen relevant, die in Vertretung anderer Personen durch Verwendung einer Vollmacht erfolgt. In diesem Fall bietet diese Domain mit dem Unternehmensregister eine von mehreren Quellen, aus denen Vollmachten-Informationen bezogen werden können.

SZRB-Domain

Der Bereich der Stammzahlenregisterbehörde (SZRB) ist wie die Statistik-Austria-Domain bei einer Verwendung von Vollmachten zur Anmeldung an Applikationen in Vertretung anderer Personen relevant. In diesem Fall bietet diese Domain mit dem bilateralen Register für Vollmachten eine von mehreren Quellen, aus denen Vollmachten-Informationen bezogen werden können.

USP/PVP-Domain

Das Unternehmensserviceportal (USP) und das Portalverbundprotokoll (PVP) sind bereits existierende Strukturen, die zur Registrierung von Service Providern im ID Austria System verwendet werden können. Die USP-Domain und die PVP-Domain stellen somit Komponenten bereit, über die sich Service Provider registrieren können[77] und fungieren zudem als Quelle für Vollmachten-Informationen.

BMDW-Admin-Domain

Diese (derzeit noch nicht umgesetzte, aber geplante) Funktionalität soll dabei helfen, das von der DSGVO vorgeschriebene Auskunftsrecht für Betroffene umzusetzen bzw abzuwickeln. Eine für diese Funktion dementsprechend notwendige Entität ist zunächst ein DSGVO-Admin, der im Umfeld des BMDW angesiedelt ist und an den sich *E-ID-Inhaber* mit einem Auskunftsbegehren gemäß der DSGVO wenden können. Der DSGVO-Admin interagiert in dieser BMDW-Admin-Domain mit dem DSGVO-Admin-Client. Dabei handelt es sich um eine technische Komponente, die den Bezug der benötigten Daten aus der E-ID-Frontend-Domain gewährleistet.

[77] Siehe hierzu insbesondere 3.2.1.

3.2 Datenverarbeitungstätigkeiten im ID Austria System

3.2.1 Registrierung und Akkreditierung der Service Provider

Das ID Austria System ermöglicht die Einbindung von Service Providern. Als Service Provider wird ein Anwendungsendpunkt bezeichnet, welcher durch einen Service Owner (zB Unternehmen, Verein, Behörde) betrieben wird. Der Service Provider ermöglicht die Anmeldung von Benutzer*innen in einer Anwendung (wie zB Web-Applikationen) über das ID Austria System. Die ID Austria fungiert dabei als Identity Provider (IDP), welcher den Service Ownern für ihre Services bzw Anwendungen verschiedene Authentifizierungsmöglichkeiten zur Verfügung stellt.[78]

Damit Service Owner das ID Austria System zur Identifikation von Benutzer*innen für ihre digitalen Anwendungen verwenden können, ist zunächst die Registrierung des für den jeweiligen Service Provider verantwortlichen Service Owners erforderlich.[79] Erst nach erfolgreicher Registrierung des Service Owners kann dieser in weiterer Folge auch seine Service Provider (bzw Applikationen) registrieren und akkreditieren lassen. Ein Service Owner kann dabei auch mehrere Service Provider bzw Anwendungen akkreditieren lassen.

Die Registrierung und Akkreditierung der Service Owner und ihrer Service Provider soll das Vertrauen in das ID Austria System insgesamt erhöhen. So soll durch den vorgesehenen Registrierungs- und Akkreditierungsprozess kontrolliert werden, dass Service Provider nur jene Daten (bzw Attribute) erhalten, die sie für das angebotene Service auch tatsächlich benötigen, um die Verhältnis- bzw Zweckmäßigkeit der jeweiligen Verarbeitung aufrechtzuerhalten. Zudem sollen Service Provider mit unlauteren Agenden von der Nutzung des Systems ausgeschlossen werden.[80]

Hierzu sieht § 18 Abs 2 E-GovG vor, dass der BMI (Bundesminister für Inneres) dazu ermächtigt ist, *Dritten* die Nutzung des E-ID-Systems nicht zu eröffnen oder zu unterbinden, wenn Anhaltspunkte dafür bestehen, dass diese die ihnen zur Verfügung gestellten personenbezogenen Daten nicht gemäß dem Grundsatz nach Treu und Glauben und auf rechtmäßige Weise verarbeiten werden. Zu diesem Zweck ist das BMI auch berechtigt, im Rahmen der Registrierung und Akkreditierung von privaten Service Provider Informationen über nicht getilgte rechtskräftige strafrechtliche Verurteilungen sowie die genaue Bezeichnung des Gewerbes abzufragen. Ferner dürfen jene Daten, die dem *Dritten* (SP bzw SO) im Auftrag des *E-ID-Inhabers* übermittelt werden, ausschließlich für die im Rahmen der Registrierung und Akkreditierung bekannt- und glaubhaft gemachten eigenen Zwecke verarbeitet werden.

Der Registrierungs- und Akkreditierungsprozess der Service Owner bzw Service Provider erfolgt über das Service Provider-Register-Service (SPRS) der ID Austria. Der Zugriff auf diese Applikationsverwaltungsplattform wird über die bereits existierende Infrastruktur des Unternehmensserviceportals (USP) sowie des Portalverbundprotokoll (PVP) ermöglicht.[81] Die

[78] Siehe hierzu Kapitel 3.2.3 zur „Verwendung des E-ID zur Nutzung von Anwendungen".
[79] Siehe § 4 Abs 3 E-GovG.
[80] Siehe § 18 Abs 2 E-GovG; Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 18.
[81] Siehe Unternehmensserviceportal, https://www.usp.gv.at/ (abgerufen am 22. 04. 2022); Portalverbund: Arbeitsgruppe Integration/Zugänge (AG-IZ), Portalverbund, https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).

zuständige Stelle für die Akkreditierung privater Service Provider ist das Bundesministerium für Inneres (BMI). Das Bundesrechenzentrum (BRZ) fungiert als Dienstleister.[82] Das BRZ stellt das SPRS zur Registrierung der Service Provider zu Verfügung. Das Portal ist für private und behördliche Provider anders ausgestaltet; es handelt sich um eine Applikation, die je nach Zugriffsart unterschiedlich aussieht. Dabei wird zwischen privatwirtschaftlichen und öffentlichen (bzw behördlichen) Service Ownern differenziert. So können Service Owner des öffentlichen Sektors ihre Registrierung über die behördenübergreifende Anwendung des Portalverbunds vornehmen.[83] Privatwirtschaftliche Service Owner haben wiederum die Möglichkeit über das Unternehmensserviceportal (USP) auf das SPRS zuzugreifen.

Während sowohl private als auch öffentliche Service Provider in einem ersten Schritt registriert werden müssen, gibt es hinsichtlich der anschließenden Akkreditierung kategorische Unterschiede.[84] So wird die Eröffnung der Nutzung der ID Austria im Fall privatwirtschaftlicher Service Provider manuell geprüft, wohingegen behördliche Service Provider automatisch freigeschalten werden bzw bereits im Zuge der Ausstattung mit einem bereichsspezifischen Personenkennzeichen (bPK) einer Vorabkontrolle unterliegen. Es erfolgt kein gesonderter Akkreditierungsschritt seitens der SZRB. Die Registrierungsdaten der Provider des öffentlichen Sektors werden nachträglich (ex post) stichprobenartig überprüft. Eine Maßnahmenergreifung erfolgt bei entsprechender Beobachtung möglichen Missbrauchs oder sicherheitskritischer Ereignisse.[85]

3.2.1.1 Registrierung

Die Registrierung und Verwaltung öffentlicher (bzw behördlicher) Service Provider durch oder im Auftrag des Service Owners, soll über den Portalverbund erfolgen.[86] Der Portalverbund ist eine breit verwendete[87] staatliche Anwendung bzw Verknüpfung behördenübergreifender Web-Applikationen mit einer Vereinheitlichung von Zugriff[88] und Rechteverwaltung[89], wobei insb auch einheitliche Sicherheitsstandards im Rahmen einer Vereinbarung vorgegeben sind.[90]

Als behördenübergreifende Webanwendung bietet der Portalverbund für öffentliche Service Owner Zugriff auf das SPRS des ID Austria-Systems zur Verwaltung ihrer jeweiligen Services bzw

[82] Gem § 18 Abs 3 E-GovG ist das BMI im Einvernehmen mit dem BMDW dazu ermächtigt, nähere Bestimmungen über die Vorgangsweise bei der Akkreditierung weiterer anderer *Dritter* durch Verordnung festzulegen.
[83] Vgl https://eid.egiz.gv.at/anbindung/registrierung/registrierung-von-behoerdlichen-service Providern/ (abgerufen am 22. 04. 2022).
[84] Die vorliegenden Ausführungen beziehen sich auf die Akkreditierung privatwirtschaftlicher Service Provider. Eine Prüfung der Akkreditierung öffentlicher bzw behördlicher Service Provider liegt nicht im Fokus der Datenschutz-Folgenabschätzung.
[85] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner (2021) 18.
[86] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner.
[87] Siehe die angebundenen Anwendungen unter: https://portal.lfrz.at/at.gv.lfrz.pai-p/application_summary (abgerufen am 22. 04. 2022).
[88] Single Sign On: vgl *Arbeitsgruppe Integration/Zugänge (AG-IZ)*, Portalverbund, https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).
[89] Single Point of Administration: vgl *Arbeitsgruppe Integration/Zugänge* (AG-IZ), Portalverbund, https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).
[90] Vgl *Arbeitsgruppe Integration/Zugänge (AG-IZ)*, Portalverbund, https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).

Anwendungen.[91] Dies umfasst sowohl die neue Registrierung von Anwendungen als auch die Aktivierung bzw Deaktivierung registrierter Anwendungen sowie die Konfiguration und Änderung von Anwendungsparametern.[92]

Ähnlich wie behördliche Provider über den Portalverbund, können private Service Provider über das bereits bestehende USP registriert werden und damit auf das SPRS des ID Austria Systems zugreifen.[93] Die Registrierung einer natürlichen Person (und damit verknüpft eines Unternehmens)[94] im USP erfolgt entweder mittels Handy-Signatur (künftig mit der ID Austria) oder mit privatem FinanzOnline-Zugang.[95]

Im Zuge der Registrierung und Akkreditierung kann es zur Verarbeitung der folgenden Daten der Service Owner (SO) und Service Provider (SP) kommen:[96]

Daten der Service Owner:

- Typ des Antragstellers
- Organisationskennzeichen (OKZ)
- Name
- Unternehmensgegenstand/Vereinszweck
- Rechtsform
- FB-Nr/Vereinszahl/ERsB-Ordnungsnummer
- GISA-Zahl[97]
- ÖNACE (Zuordnung zu mehreren Wirtschaftszweigen bzw -branchen möglich)
- Pool an *Verantwortlichen*[98] (mit Geburtsdatum, Person-Rolle, Anrede, Akademischer Grad, Vor- und Nachname, Geburtsdatum, Telefonnummer, E-Mail-Adresse); im Fall privater Service Provider muss zumindest ein *Verantwortlicher* gespeichert werden; die Angabe der E-Mail-Adresse sowie der Telefonnummer (des Unternehmens oder Vereins) ist verpflichtend. Für Behörden wird hingegen keine natürliche Person als *Verantwortlicher* gespeichert.

[91] Siehe *Arbeitsgruppe Integration/Zugänge (AG-IZ)*, Portalverbund, https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22. 04. 2022).
[92] Als Rechtsgrundlage zur Registrierung behördlicher Service Provider dient § 10 Abs 1 S 2 E-GovG. Für weitere Informationen zum Registrierungsprozess von öffentlichen bzw. behördlichen Service Providern siehe https://eid.egiz.gv.at/anbindung/registrierung/registrierung-von-behoerdlichen-service Providern/ (abgerufen am 22. 04. 2022).
[93] https://www.usp.gv.at/ (abgerufen am 22. 04. 2022).
[94] Die Registrierung natürlicher Personen als Service Provider ist derzeit nicht als Privatperson, sondern nur als Einzelunternehmen möglich.
[95] Siehe https://www.usp.gv.at/ (abgerufen am 22. 04. 2022). Handy-Signatur-Nutzern wird nach der Einführung der ID Austria ein vereinfachter Umstieg auf das E-ID-System ermöglicht.
[96] Siehe hierzu auch § 18 Abs 5 E-GovG.
[97] Mit der sog GISA-Zahl kann die Gewerbeberechtigung abgefragt werden.
[98] Der Begriff „Verantwortlicher" bezieht sich hier auf § 9 VStG und wird nicht iSd Definition in Art 4 Z 7 DSGVO verwendet.

- Pool an Kontaktpersonen (ohne Geburtsdatum, jedoch mit Rolle, Anrede, Akademischer Grad, Vorname, Telefonnummer, E-Mail-Adresse); im Fall öffentlicher (bzw behördlicher) Service Owner dürfen keine Personen eingetragen werden, sondern nur Organisationseinheiten. Wenn es sich um Organisationseinheiten handelt, dann werden wiederum die folgenden Daten verarbeitet: Bezeichnung der Organisationseinheit, Telefonnummer, E-Mail-Adresse.
- Pool an Adressen mit jeweils folgenden Eigenschaften: Rolle, Firmensitz, Zustelladresse (Straße, HausNr, Stiege, Türnummer, PLZ, Ort, Staat)
- Logos-Pool (Mime-Type, Auflösung, Dark/Light Theme)

Daten der Service Provider:

Basisinformationen:

- Art des Service Providers (Ist der Service Provider öffentlich oder privat?)
- URL (URL auf Website des Service oder der Info-Page in App)
- App-ID (Entity-ID [SAML2] bzw Client-ID [OIDC])[99]
- SP-Version (URN) (Version des Service Providers)
- FriendlyName (Kurzbeschreibung des Providers wie bspw FinanzOnline)
- Datenschutz-Policy URL (URL der Datenschutzpolicy beim SP)
- Flag Testidentitäten (Unterstützung Testidentitäten ja/nein)
- Flag eIDAS (Unterstützung eIDAS ja/nein)
- Timeout last E-ID Login (Wie lange darf die letzte Anmeldung auf diesem Gerät mit der E-ID zurückliegen; längster zurückliegender Zeitpunkt der letzten E-ID Anmeldung; für vereinfachte Weiterverwendung).
- Zuordnung von Logos (Logos des SP zur Anzeige in der Anmeldemaske)

Rechtliche Informationen:

- Zuordnung eines *Verantwortlichen* gem § 9 VStG
- Strafregister-Auszug der *Verantwortlichen* geprüft (Zeitstempel)[100]
- Zuordnung von Kontaktpersonen

[99] Hierbei handelt es sich um zwei technische Identitätsmanagementprotokolle; die ID dient der Unterscheidung der Service Provider.
[100] Eine derartige Überprüfung findet pro (neuem) Antrag statt.

- Zuordnung von Adressen
- Zweck der Nutzung des E-ID Systems (Angaben zu welchem Zweck das E-ID System insgesamt genutzt wird; Begründung auf Ebene der Anwendung)
- Rechtsgrundlage bzw Begründung für Attribute (inkl Beschreibung der Applikation); im Fall öffentlicher Service-Provider können Attribute aus Registern, die der Stammzahlenregisterbehörde rechtlich (gesetzliche Grundlage) und technisch zugänglich sind, über das E-ID-System bezogen werden, wenn der öffentliche Service Provider diese Daten in seiner Datenverarbeitung verarbeiten darf. Im Fall privater Service Provider ist eine Begründung anzugeben, warum bzw zu welchem Zweck das einzelne Attribut verarbeitet wird.
- Bestätigung der Einhaltung gesetzlicher Bestimmungen: „Hiermit bestätige ich die Einhaltung der Bestimmungen der Datenschutzgrundverordnung (DSGVO). Die erhaltenen Daten werden ausschließlich entsprechend der gesetzlichen Bestimmungen und nach Treu und Glauben (§ 18 Abs. 2 E-GovG) verarbeitet. Ich nehme zur Kenntnis, dass die Nutzung des E-ID Systems nur für die glaubhaft gemachten eigenen Zwecke in Anspruch genommen werden darf; die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck.“ Dies ist vom Service Owner beim Eintragen zwingend zu aktivieren, sonst darf das Formular nicht abgeschickt bzw nicht entgegengenommen werden; das Absenden mit dieser Zustimmung ist für die Behörde nachvollziehbar zu persistieren, inkl der Information, welcher Version zugestimmt wurde (falls später ein anderer Text eingetragen wird, dem zugestimmt wird).
- Bestätigung der Einhaltung gesetzlicher Bestimmungen: „Ich habe die mir im Falle einer Freischaltung zum E-ID System obliegenden Pflichten zur Kenntnis genommen." Dies ist vom Service Owner beim Eintragen zwingend zu aktivieren, sonst darf das Formular nicht abgeschickt bzw nicht entgegengenommen werden; das Absenden mit diesem Wert ist für die Behörde nachvollziehbar zu persistieren, inkl der Information, welcher Version zugestimmt wurde (falls später ein anderer Text eingetragen wird, dem zugestimmt wird).[101]
- allfällige Gründe, die Treu und Glauben entgegenstehen
- Behörden-internes mehrzeiliges Kommentarfeld (zB „abgelehnt mit Bescheid Nr. x vom d.m.j“)

Identifikatoren:

- Bereichsspezifisches Personenkennzeichen (bPK) des Service Providers; (Kürzel aus der E-Gov-BerAbgrVO,[102] Sub-Bereich, Quelle)[103]; Liste unverschlüsselter bPKs von öffentlichen Bereichen inkl Bereichskürzel und Sub-Bereich (nur für öffentliche Service Owner relevant; dürfen nicht an

[101] Siehe hierzu § 18 Abs (7) E-GovG; sofern *Dritte* die Nutzung des E-ID Systems eröffnet wurde, haben diese dem Bundesminister für Inneres unverzüglich zu melden, wenn sich ein glaubhaft gemachter Zweck oder der *Verantwortliche* ändert oder *Dritte* die glaubhaft gemachten Zwecke nicht mehr verfolgen wollen oder dürfen.

[102] Verordnung des Bundeskanzlers, mit der staatliche Tätigkeitsbereiche für Zwecke der Identifikation in E-Government-Kommunikationen abgegrenzt werden (E-Government-Bereichsabgrenzungsverordnung – E-Gov-BerAbgrV); StF: BGBl. II Nr. 289/2004.

[103] Diese werden idealerweise statisch durch die Zuordnung des Users an einen SO gesetzt, oder abgeleitet von Anmeldung.

private SP weitergegeben werden). Liste von Datensätzen zur Berechnung von weiteren bPKs für den öffentlichen Bereich.

- Liste unverschlüsselter bPKs von privaten Bereichen inkl Quelle und Identifikator; Liste von Datensätzen zur Berechnung von weiteren bPKs für den privaten Bereich
- Liste (verschlüsselter) Fremd-bPK von Öffentlichen inkl Bereichskürzel, Sub-Bereich und Verwaltungskennzeichen (VKZ) oder Service-ID;[104] Liste von Datensätzen zur Berechnung weiterer verschlüsselter Fremd-bPKs für den öffentlichen Bereich[105]

Vollmachten:

- Flag Vollmachten aktiviert (Unterstützung Vollmachten per SAML2/OIDC ja/nein)
- Flag nur Vollmachten (Anmeldung ausschließlich mit Vollmachten)
- Flag Multivollmachten aktiviert (Nachladen von Vollmachten für natürliche Person erlaubt ja/nein)
- Multivollmachten Zertifikat (Client-Zertifikat für Multivollmachten Schnittstelle)
- Liste zulässiger Profile[106]

Attribute:

- Liste der Attribute, die vonseiten der Service Provider verarbeiten werden[107]

SAML2 Metadaten:

- entityID (Eindeutiger Identifier der Applikation)
- KeyDescriptor: X509 Zertifikate für Encryption/Signaturen, [use] (Verwendung für Signatur-Verifizierung oder Verschlüsselung), ds:KeyInfo (Zertifikatdaten).
- AssertionConsumerService: Rücksprung auf SP, [Binding] (Kommunikationsart / SAML2 Binding), [Location] (URL auf den SP Endpunkt für Assertions), [index] (Index für Auswahl im AuthnRequest)

OIDC Metadaten:

[104] Diese dürfen an private SP weitergegeben werden; es ist aber zu prüfen, auf welche verschlüsselte bPK der SP zugreifen darf.
[105] Mit verschlüsselten bPKs können Applikationen aus unterschiedlichen Bereichen zusammenarbeiten und dieselbe Person identifizieren.
[106] Siehe hierzu das „Online-Vollmachten Service (OVS)“ der Stammzahlenregisterbehörde, https://vollmachten.stammzahlenregister.gv.at/mis/ (abgerufen am 22. 04. 2022).
[107] Als Attribute gelten zB Informationen wie das (Nicht-)Vorhandensein eines Führerscheins (bzw einer Lenkberechtigung) aber auch Informationen wie das Geburtsdatum.

- redirect_urls (URL auf den SP für Rücksprung)
- jwks (Encryption Zertifikat)

Apps (falls für SP verfügbar):

- Android Apps: Package Name der SP-App (eindeutiger Identifier der App auf Android-Systemen); SHA256 Fingerprint des Zertifikates der App
- IOS Apps: Bundle Identifier der SP App (eindeutiger Identifier der App auf iOS-Systemen)

Im Zuge der Registrierung der Service Owner und Service Provider erhält und verarbeitet das ID Austria System somit eine Reihe technischer und organisatorischer Informationen. Basierend auf diesen Informationen können für die Service Owner und ihre Applikationen verschiedene Policies definiert werden, wie zB die Befugnis zur Abfrage von unverschlüsselten bzw verschlüsselten bereichsspezifischen Personenkennzeichen (bPKs) diverser Bereiche oder zur Verwendung bestimmter Attribute aus verschiedenen behördlichen oder privaten Registern.[108]

Im Zusammenhang mit der Verwaltung der Kategorien von Attributen werden wiederum die folgenden Daten verarbeitet:

Generelle Daten:

- Nachname
- Vorname
- Geburtsdatum
- Bereichsspezifische Personenkennzeichen
- Verschlüsselte Bereichsspezifische Personenkennzeichen / Fremd-bPKs

Weitere Daten:

- Authentifizierungslevel der Person (Bürger*in)
- Authentifizierungsmethode der Person (Bürger*in)
- Authentifizierungsstatus der Person (Bürger*in)
- eID-Herausgebernation
- Bereich und Typ des bereichsspezifischen Personenkennzeichens
- Online-Personenbindung

[108] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 17.

- URL Bürgerkartenumgebung
- eID-Signatur-Zertifikat bei Authentifizierung

Allgemeine Vollmacht-Informationen:

- Vollmachtentype
- Vollmachtentype-OID
- Access Token zur Backendabfrage von Vollmacht

Juristische Person wird vertreten:

- Stammzahltyp der vertretenen juristischen Person
- Stammzahl der vertretenen juristischen Person
- Name der juristischen Person

Natürliche Person wird vertreten:

- Bereichsspezifisches Personenkennzeichen der vertretenen Person
- Liste von bereichsspezifischen Personenkennzeichen der vertretenen Person
- Verschlüsselte Fremd-bPKs der vertretenen Person
- Vorname der vertretenen natürlichen Person
- Nachname der vertretenen natürlichen Person
- Geburtsdatum der vertretenen natürlichen Person

Berufsmäßige Parteienvertreter*innen:

- Kennzeichnung berufsmäßiger Parteienvertreter*innen
- Beschreibung der Eigenschaft berufsmäßiger Parteienvertreter*innen

Auf dieser Basis wird verwaltet, welche Attribute und, damit verbunden, welche Anwendungen die ID Austria dem Service Owner (bzw dessen Service Providern) bereitstellt bzw ermöglicht. Über den minimalen Datensatz ([v]bPKs, Name, Geburtsdatum) hinausgehende Attribute werden dabei aus behördlichen oder privaten Registern bezogen.[109]

[109] Vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper für Service Owner 17. Hierzu können künftig zB auch Register über Mitgliedschaften in Vereinen oder Clubs zählen. Konkrete Use Cases liegen aktuell jedoch noch nicht vor.

3.2.1.2 Akkreditierung

In Verbindung mit der Registrierung und Eingabe der notwendigen Daten erfolgt weiters die Akkreditierung des Service Providers.[110] Diese ist grundsätzlich bei jeder Neuregistrierung erforderlich. Zudem kann die Anpassung eines bestehenden Service Providers eine Neuakkreditierung notwendig machen, sofern die Änderungen zuvor akkreditierte Daten betreffen. Im Zuge der Akkreditierung werden die verschiedenen technischen und organisatorischen Informationen der Provider überprüft.

Die vorliegenden Ausführungen beziehen sich insb auf die Akkreditierung privater Service Provider. Während die Akkreditierung der privatwirtschaftlichen Service Provider persönlich bzw händisch erfolgt, werden öffentliche (bzw behördliche) Service Provider - wie bereits erwähnt - automatisch für die Verwendung der ID Austria sowie etwaiger Attribute freigeschaltet. Es gibt jedoch die Möglichkeit einer ex post Kontrolle. Die Registrierungsdaten der öffentlichen Service Provider werden im Nachhinein stichprobenartig überprüft. Die Aktivierung der Anwendung eines (privaten) Service Providers kann jedenfalls nur nach positiver Akkreditierung erfolgen.

Im Fall öffentlicher Service-Provider können Attribute aus Registern, die der Stammzahlenregisterbehörde rechtlich (gesetzliche Grundlage) und technisch zugänglich sind, über das E-ID-System bezogen werden, wenn der öffentliche Service Provider diese Daten in seiner Datenverarbeitung verarbeiten darf. Eine Vorabkontrolle oder Überprüfung der Rechtsgrundlagen auf Richtigkeit bzw Plausibilität erfolgt nicht.[111] Ein Grund zur Stilllegung des Accounts eines behördlichen Providers wäre bspw Missbrauch oder ein Cyberangriff.

Im Fall der privaten Service Provider sind Begründungen dafür anzugeben, warum bzw zu welchem Zweck einzelne Attribute gebraucht werden. Dies inkludiert auch eine Beschreibung der jeweiligen Applikation. Ferner dürfen *Dritte* die personenbezogenen Daten im konkreten Fall nur für die glaubhaft gemachten eigenen Zwecke verarbeiten. Die Service Provider haben hierzu im SPRS anzugeben, welche Attribute sie wozu für welche Anwendungen benötigen. Aufgrund des Freitext-Felds können noch zusätzlich personenbezogene Daten anfallen.

Gem § 18 Abs 2 E-GovG hat der BMI die Nutzung des E-ID Systems einem *Dritten* dann nicht zu eröffnen bzw zu unterbinden, wenn Anhaltspunkte dafür bestehen, dass der *Dritte* die ihm zur Verfügung gestellten personenbezogenen Daten nicht gemäß dem Grundsatz nach Treu und Glauben und auf rechtmäßige Weise verarbeitet hat.

Die Prüfung nach Treu und Glauben erfolgt primär über die Strafregisterabfrage. Zudem ist ein Eingabefeld vorgesehen, in das die Service Provider Gründe bzw Hindernisse eintragen können, die einer Eröffnung potentiell entgegenstehen.

Wie oben bereits aufgelistet, werden im Zuge der Registrierung und Akkreditierung darüber hinaus die folgenden Bestätigungen zur Einhaltung gesetzlicher Bestimmungen eingeholt:

- „Hiermit bestätige ich die Einhaltung der Bestimmungen der Datenschutzgrundverordnung (DSGVO). Die erhaltenen Daten werden ausschließlich entsprechend der gesetzlichen

[110] Rechtsgrundlage für die Registrierung behördlicher Provider ist § 10 Abs 1 2. Satz E-GovG (es erfolgt kein gesonderter Akkreditierungsschritt seitens der SZRB).
[111] Allerdings wird bereits im Zuge der Ausstattung des behördlichen Providers mit bereichsspezifischen Personenkennzeichen (bPK) eine Überprüfung durch die SZRB vorgenommen.

Bestimmungen und nach Treu und Glauben (§ 18 Abs. 2 E-GovG) verarbeitet. Ich nehme zur Kenntnis, dass die Nutzung des E-ID Systems nur für die glaubhaft gemachten eigenen Zwecke in Anspruch genommen werden darf; die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck."

– „Ich habe die mir im Falle einer Freischaltung zum E-ID System obliegenden Pflichten zur Kenntnis genommen."

Diese Bestätigungen sind vom Service Owner im Zuge der Registrierung und Akkreditierung zwingend in Form eines opt-in Mechanismus abzugeben; das Formular darf sonst nicht abgeschickt werden. Die Bestätigung inkl der Information, welcher Version zugestimmt wurde, ist für die Behörde nachvollziehbar zu persistieren.

Wurde die Nutzung bereits eröffnet, sind *Dritte* verpflichtet, jeden Umstand bekanntzugeben, der einer Nutzung entgegensteht. Ferner ist der akkreditierte *Dritte* auch gem § 18 Abs 7 E-GovG dazu verpflichtet, unverzüglich zu melden, dass sich der von ihm glaubhaft gemachte Zweck oder der *Verantwortliche* gem § 9 VStG geändert haben oder er die von ihm glaubhaft gemachten Zwecke nicht mehr verfolgen will oder darf.

Zum Zweck der Eröffnung der Nutzung des ID-Austria Systems ist das BMI zudem dazu berechtigt, Informationen über nicht getilgte rechtskräftige strafgerichtliche Verurteilungen von *Verantwortlichen* abzufragen. Als Nicht-Eröffnungsgrund werden im E-GovG unter § 18 Abs 2 insbesondere der widerrechtliche Zugriff auf ein Computersystem gem § 118a StGB, die Verletzung des Telekommunikationsgeheimnisses gem § 119 StGB und das missbräuchliche Abfangen von Daten gem § 119a StGB genannt.

Im Zuge der Akkreditierung werden die Daten des Service Providers auf Korrektheit und Plausibilität geprüft. Wenn die gesetzlichen Vorgaben nicht erfüllt sind, also bspw ein entsprechender Strafregistereintrag vorliegt, ist dies ein Grund zur Nicht-Eröffnung. Liegen alle Angaben wie erforderlich vor, erfolgt die Freischaltung des Service Providers für die Verwendung der ID Austria.

Die entsprechende Prüfung erfolgt einmal zu Beginn; eine wiederholte periodische und technische automatisierte Abfrage bzw Prüfung ist nicht vorgesehen. Der Fokus der Akkreditierung liegt im Wesentlichen auf dem angegebenen Verwendungszweck und ob dieser mit der gewerblichen Ausrichtung des Unternehmens übereinstimmt. Eine inhaltliche Prüfung der Datenschutzerklärung des privaten Service Providers bzw Unternehmens wird nicht durchgeführt; es wird lediglich darauf geachtet, ob diese grundsätzlich vorliegt.

Sollten im Fall eines privaten Service Providers Hinweise auftreten, dass dieser nicht mehr vertrauenswürdig ist, wäre dies ein Grund für die Stilllegung. Die Kommunikation des Ergebnisses einer negativen Akkreditierung im Sinne einer Nicht-Eröffnung der Nutzung des ID Austria Systems erfolgt in formalrechtlicher Hinsicht via Bescheid.

Wenn ein Service Owner über einen Zeitraum von fünf Jahren das ID Austria System nicht nutzt, also innerhalb dieses Zeitraums keine akkreditierten Service Provider hatte, weil diese bspw stillgelegt

wurden, werden sämtliche Daten des privaten Service Owners und seiner Service Provider (automatisch) gelöscht.[112]

Darüber hinaus ist der BMI schließlich auch dazu ermächtigt, im Einvernehmen mit dem BMDW nähere Bestimmungen über die Vorgangsweise in Akkreditierungsprozessen durch Verordnungen festzulegen. Nach § 18 Abs 3 E-GovG könnten sich diese künftig insbesondere darauf beziehen, inwieweit neben Unternehmen und Vereinen auch andere Teilnehmer*innen des Unternehmensserviceportals oder andere *Dritte* registriert werden können, sowie inwiefern *Dritte* sowohl die Kosten für die Eröffnung der Nutzung als auch für die Nutzung des E-ID Systems zu ersetzen haben.

[112] Siehe hierzu die Normierung der Frist über § 18 Abs 6 E-GovG.

3.2.2 Registrierung der Benutzer*innen

Um einen elektronischen Identitätsnachweis bzw E-ID zu erhalten, müssen Benutzer*innen bzw Bürger*innen einen Registrierungsprozess durchlaufen. Im Rahmen dieses E-ID-Registrierungsprozesses werden die jeweiligen Bürger*innen von E-ID-Werber*innen zu *E-ID-Inhabern*. Nach dem erfolgreichen Abschluss des gesamten E-ID-Registrierungsprozesses steht den Bürger*innen ihr persönlicher E-ID bzw ID Austria zur Verwendung iSd Nutzung von Anwendungen zur Verfügung.

Die Registrierung eines E-ID kann grundsätzlich von allen natürlichen Personen, die im österreichischen Stammzahlenregister (SZR)[113] eingetragen sind, ab dem vollendeten 14. Lebensjahr vorgenommen werden, wobei es unterschiedliche Varianten gibt, um über das SZR auffindbar zu sein. Hierzu zählen einerseits natürliche Personen, die im Zentralen Melderegister (ZMR), welches alle in Österreich gemeldeten natürlichen Personen mit ihrem Hauptwohnsitz und, sofern vorhanden, mit ihrem(/ihren) Nebenwohnsitz(en) erfasst, eingetragen sind.

Andererseits können über das SZR auch jene natürlichen Personen auffindbar sein, die sich manuell im Ergänzungsregister natürliche Personen (ERnP) eintragen haben lassen (allenfalls auch im Zuge der Registrierung des E-ID). Letztendlich erfolgt eine automatische Eintragung im ERnP auch durch die Verwendung einer eIDAS-konformen ausländischen eID bei einem österreichischen Service Provider (SP).

Der E-ID-Registrierungsprozess kann dabei entweder amtswegig oder auf Verlangen der Bürger*in bei der jeweils zuständigen und hierzu ermächtigten Registrierungsbehörde beginnen.

Amtswegig startet der Registrierungsprozess von Bürger*innen im Zuge der Beantragung eines Reisepasses oder Personalausweises, unter der zwingenden Voraussetzung, dass die Bürger*in der E-ID-Registrierung hierbei nicht ausdrücklich widerspricht (Opt-out-Lösung)[114].

Unabhängig davon kann der Registrierungsprozess von Bürger*innen auch jederzeit auf deren Verlangen gestartet werden.

Personen, die die österreichische Staatsbürgerschaft nicht besitzen, können den Registrierungsprozess unter bestimmten weiteren Voraussetzungen hingegen nur auf Verlangen starten.

[113] Das Stammzahlenregister ist gem § 2 Z 9 E-GovG: „Ein Register, das die für die eindeutige Identifikation von Betroffenen verwendeten Stammzahlen enthält bzw. die technischen Komponenten zur Ableitung von Stammzahlen im Bedarfsfall besitzt“; das SZR liegt gem § 7 Abs 1 E-GovG im Verantwortungsbereich der Stammzahlenregisterbehörde (SZRB), welche der Bundesminister für Digitalisierung und Wirtschaftsstandort (BMDW) ist; das SZR wird im Auftrag der SZRB vom BMI betrieben.

[114] Im Rahmen der (nachfolgend näher ausgeführten) Registrierungsvariante C, D und E erhält der *E-ID-Werber* von den Behördenmitarbeiter*innen einerseits einen ID Austria-Behördenausdruck, welcher die für den erfolgreichen Abschluss der betreffenden Registrierungsvariante wesentlichen Angaben (Freischaltcode und Widerrufs-Passwort) sowie eine Belehrung zur Möglichkeit des jederzeitigen Widerrufs der ID Austria beinhaltet. Andererseits erhält der *E-ID-Werber* auch eine ID Austria Broschüre, die neben allgemeinen Informationen zur ID Austria auch einen Hinweis auf die Opt-out Möglichkeit beinhaltet. Darüber hinaus befindet sich ein Hinweis auf die Opt-out Möglichkeit (bzw deren Bestätigung) auch direkt auf dem Pass- bzw Personalausweisantrag des *E-ID-Werbers*.

3.2.2.1 Architekturüberblick des E-ID-Registrierungsprozesses

Der E-ID-Registrierungsprozess erfolgt über definierte organisatorische Prozesse und technische Komponenten, die in der Registration-Domain angesiedelt sind. Die Registration-Domain und ihre Komponenten werden vom BMI bereitgestellt bzw im Auftrag des BMDW als SZRB vom BMI betrieben. Die Registration-Domain verfügt über eine Schnittstelle zur User-Domain, da die Benutzer*innen mit ihren Endgeräten mit Komponenten der Registration-Domain für den erfolgreichen Abschluss des E-ID-Registrierungsprozesses interagieren müssen. Die Registration-Domain verfügt über weitere Schnittstellen zur Backend-Domain und zur VDA-Domain. Die Backend-Domain wird ebenso vom BMI im Auftrag des BMDW als SZRB betrieben und beinhaltet unter anderem das für die Registrierung einer persönlichen ID Austria notwendige Stammzahlenregister (SZR). Die VDA-Domain repräsentiert hingegen den Bereich des *Vertrauensdienstanbieters* (VDA), der im Zuge der Registrierung einer E-ID bzw ID Austria ein qualifiziertes Signaturzertifikat für die Benutzer*innen ausstellt.

3.2.2.2 Registrierungsprozess

Im Rahmen der Registrierung werden zusammengefasst folgende Schritte, durch deren erfolgreichen Abschluss den Benutzer*innen ihr persönlicher E-ID bzw ID Austria zur Verwendung iSd Nutzung von Anwendungen zur Verfügung steht, durchgeführt:

Identitätsfeststellung: Hierbei wird die Identität von Benutzer*innen bzw E-ID-Werber*innen, ua durch persönliches Vorweisen eines Lichtbildausweises (Reisepasses, Personalausweises, Führerschein) von der hierzu ermächtigten Registrierungsbehörde eindeutig festgestellt.

Erstellung des E-ID: Hierbei wird im ID Austria System der E-ID bzw ID Austria der E-ID-Werber*innen angelegt. Unter anderem umfasst dies die Ausstellung eines sogenannten qualifizierten Signaturzertifikats für die betreffende Person und die Verknüpfung dieses Zertifikats mit der (verschlüsselten) Stammzahl der E-ID-Werber*innen über die erstellte und signierte Datenstruktur qcBind bzw mittels kryptographischer Bindung.

Aufgrund der Identitätsdaten der E-ID-Werber*innen (einzelne Registrierungsdaten: Vor- und Nachname, Geburtsdatum, Geburtsort, Geschlecht und das bPK) hat die Stammzahlenregisterbehörde (SZRB) die Stammzahl der E-ID-Werber*innen zu ermitteln und diese in verschlüsselter Form an den qualifizierten *Vertrauensdiensteanbieter* (VDA) zu übermitteln. Der VDA stellt daraufhin das qualifizierte Zertifikat für eine elektronische Signatur aus, das mit der Personenbindung zum E-ID der E-ID-Werber*innen verbunden werden soll. Zusätzlich zur von der SZRB ermittelten und an den VDA übermittelten Stammzahl hat die SZRB dem VDA die bereits oben angeführten Identitätsdaten (mit Ausnahme des bPK) der E-ID-Werber*innen sowie dessen Zustelladresse, soweit verfügbar die Mobiltelefonnummer und E-Mail-Adresse, und eine allfällige Beschränkung der Gültigkeitsdauer des Zertifikats zu übermitteln. Der VDA übermittelt daraufhin unverzüglich der SZRB den Identitätscode des ausgestellten Zertifikats. Mit Abschluss des gesamten E-ID- bzw ID Austria-Registrierungsprozesses kommt es letztendlich zur kryptographischen Bindung zwischen der App „Digitales Amt“ der E-ID-Werber*innen (bzw ihrer VDA-Komponente) mit der VDA-Domain, wodurch die E-ID-Werber*innen zu *E-ID-Inhabern* werden und die persönliche ID Austria bzw E-ID in der betreffenden App aktiviert ist.

Registrierung von Authentifizierungsfaktoren: Hierbei werden die Benutzer*innen mit Authentifizierungsfaktoren (Zertifikaten) ausgestattet, mit Hilfe derer sich der jeweilige *E-ID-Inhaber* in weiterer Folge zur Verwendung seiner E-ID bzw ID Austria im ID Austria System authentifizieren kann. Die Authentifizierungsfaktoren umfassen ein geheimes Passwort und ein mobiles Endnutzergerät, das kryptographisch an die ID Austria der betreffenden Person gebunden wird. Dazu wird am mobilen Gerät ein asymmetrisches Schlüsselpaar erstellt, über das ein sogenanntes Challenge-Response-Verfahren umgesetzt wird; der Zugriff auf den privaten Schlüssel wird zusätzlich über eine lokale Authentifizierungsmethode (Face-ID/Fingerprint) am mobilen Gerät geschützt.

Im Zuge des E-ID-Registrierungsprozesses werden die für die Registrierung des E-ID notwendigen Daten derselben E-ID-Werber*innen erhoben, geprüft und gegebenenfalls auch hinterlegt. Dies umfasst vor allem die Verarbeitung von Registrierungsdaten samt deren Abgleich mit Registern von Verantwortlichen des öffentlichen Bereichs zur Überprüfung der Identität und der vorgelegten Dokumente der E-ID-Werber*innen.

Folgende Daten werden im Rahmen des E-ID-Registrierungsprozesses sowie innerhalb des IDR (Identitätsdokumentenregister) von den Registrierungsbehörden verarbeitet,[115] wobei sich hinsichtlich des Umfangs der dabei zu verarbeitenden Datenmenge unter Berücksichtigung der Identität der E-ID-Werber*innen (mit oder ohne österreichische Staatsbürgerschaft), der Registrierungsart (amtswegig oder auf Verlangen) und der gewählten Registrierungsvariante, Unterschiede ergeben können:

- Vor- und Nachname
- Geburtsdatum[116]
- Geburtsort
- Geschlecht
- Staatsangehörigkeit
- bPK-ZP (Bereichsspezifische Personenkennzeichen mit Bereichserkennung ZP)[117]
- bPK-VDA (Bereichsspezifische Personenkennzeichen mit Bereichserkennung VDA)
- SZ (Stammzahl)
- Zustelladresse
- aktuelles Lichtbild
- Registrierungsdatum
- Mobil-Telefonnummer
- E-Mail-Adresse

[115] Zu einer Speicherung der betreffenden Registrierungsdaten im IDR kommt es jedoch nur, sofern jene Daten nicht bereits im IDR, ZMR oder ERnP zur Verfügung stehen.
[116] Die Kombination der Attribute Vor- und Nachname sowie Geburtsdatum trägt die Bezeichnung „Minimal Dataset“ (MDS).
[117] Für den Tätigkeitsbereich „Personenidentität und Bürgerrechte (zur Person)“.

- Registrierungsbehörde
- Identitätscode der ausgestellten Zertifikate gemäß § 4 Abs. 4 E-GovG
- Ausstellungsbehörde
- Ausstellungsstaat
- Ausstellungsdatum
- gegebenenfalls die Gültigkeitsdauer
- Dokumentenart und -nummer der vorgelegten Urkunden
- Nachweise zur eindeutigen Feststellung der Identität
- Pass- oder Personalausweisnummer
- Vorregistrierungs-ID
- Tech-ID[118]

Darüber hinaus werden im Rahmen des E-ID-Registrierungsprozesses durch das ID Austria System die folgenden Daten verarbeitet:[119]

- Username
- Signaturpasswort
- Widerrufs-Passwort
- Freischaltcode
- QR-Code
- IP-Adresse der*des Anfragenden
- Aufrufmethode (GET, HEAD, PUT)
- Zieladresse ohne HOST
- Protokoll mit Version (zB HTTP/1.1)
- Name der abgerufenen Datei und übertragene Datenmenge
- Datum und Uhrzeit des Abrufs
- Meldung, ob der Abruf erfolgreich war
- Bearbeitungsdauer des Requests in Mikrosekunden

[118] Die Tech-ID soll lediglich als technische Prozess-ID fungieren, die den jeweiligen Registrierungsprozess eindeutig identifiziert, solange kein anderer Identifikator hierfür verfügbar ist.
[119] Die Verarbeitung von personenbezogenen Daten durch die Fingerprint- bzw Face-ID-Funktion findet „nur“ lokal im hardware-secure-element des Smartphones statt; der Betrieb des E-ID Systems baut zwar zum Zweck der Registrierung und Authentifizierung wesentlich auf dieser Funktion auf, die Verarbeitung ist jedoch nicht dem ID Austria System zuzurechnen.

- Verwendeter Useragent
- Verwendete SSL-Version
- Referrer

Ferner werden im Rahmen der Registrierung auch Protokolldaten über tatsächlich durchgeführte Verarbeitungsvorgänge, die ausschließlich im Kontext mit dem E-ID-Registrierungsprozess stehen, wie insbesondere Änderungen, Abfragen und Übermittlungen, verarbeitet und drei Jahre lang aufbewahrt.[120]

Wie bereits oben angeführt, findet im Rahmen des E-ID-Registrierungsprozesses zur Überprüfung der Identität und der vorgelegten Dokumente der E-ID-Werber*innen auch ein Abgleich jener personenbezogenen Daten mit Registern von *Verantwortlichen* des öffentlichen Bereichs statt. Konkret kann die jeweils zuständige Registrierungsbehörde hierzu im Datenfernverkehr Informationen von Sicherheitsbehörden, Personenstandsbehörden[121] und Staatsbürgerschaftsbehörden[122] abfragen. Dazu zählen das Zentrale Melderegister (ZMR), das Stammzahlregister (SZR), das Ergänzungsregister natürlicher Personen (ERnP), die Personenfahndungsdatei, die Personeninformationsdatei, die Sachenfahndungsdatei, das Zentrale Personenstandsregister (ZPR), das Zentrale Staatsbürgerschaftsregister (ZSR) und das Zentrale Fremdenregister (dieses wird nur abgefragt, sofern keine österreichische Staatsbürgerschaft vorhanden ist).[123]

Soweit es sich dabei um Daten wie den Namen, Geburtsdatum, Geburtsort, Geschlecht, Staatsangehörigkeit oder die bekanntgegebene Zustelladresse handelt, verarbeitet die Registrierungsbehörde jene Daten im Rahmen der zentralen Evidenz nach dem Passgesetz, im sogenannten Identitätsdokumentenregister (IDR).

3.2.2.3 Registrierungsvarianten

Durch die nachfolgend angeführten **Registrierungsvarianten**, welche mit Ausnahme der Registrierungsvariante F („vereinfachter Umstieg“) allesamt den persönlichen Gang der E-ID-Werber*innen zur jeweiligen Registrierungsbehörde samt Beibringung eines aktuellen Lichtbildes bzw Passfotos zur persönlichen Identitätsfeststellung voraussetzen, soll den zukünftigen Benutzer*innen der Zugang zum E-ID System, durch Erhalt der ID Austria, ermöglicht werden. Für die Betriebsaufnahme der ID Austria ist insb der Prozess des sog „vereinfachten Umstiegs“ von zentraler Bedeutung.

[120] Weitere Ausführungen zur Protokollierung werden im Kapitel „Aufzeichnung von Verarbeitungsvorgängen“ festgehalten.
[121] Personenstandsbehörden (Gemeinden) führen das sogenannte Zentrale Personenstandsregister (ZPR), worin Daten über Personenstandsfälle (Geburt, Ehe, Eingetragene Partnerschaft, Tod) und damit in Zusammenhang stehende Sachverhalte (zB Namen) erfasst werden.
[122] Evidenzstellen (Gemeinden) führen das sogenannte Zentrale Staatsbürgerschaftsregister (ZSR), worin im Wesentlichen der Erwerb der österreichischen Staatsbürgerschaft und deren Verlust sowie die ausgestellten Staatsbürgerschaftsnachweise erfasst werden.
[123] Siehe hierzu auch das Elektronische Kriminalpolizeiliche Informationssystem (EKIS) und die davon umfassten Register; https://www.bmi.gv.at/402/ekis.aspx (abgerufen am 22. 04. 2022).

A. **Vorregistrierung mit der Dokumentennummer über die App „Digitales Amt“**

Für diese Registrierungsvariante ist das Vorhandensein der bereits auf dem Mobiltelefon der E-ID-Weber*innen installierten App „Digitales Amt“ erforderlich. Die E-ID-Werber*innen führen zunächst von zu Hause aus eine Vorregistrierung durch. Dazu muss mit einem Zweitgerät (zB Laptop) die Website des VDA aufgerufen werden, um darin den ersten Akt der Vorregistrierung zu setzen. Dieser inkludiert die Angabe des MDS (Minimal Dataset), einer Dokumentennummer (österreichische Pass- oder Personalausweisnummer), eines Widerrufspassworts, der Erteilung der hierfür erforderlichen Zustimmungen (Signaturvertrag, AGB, Datenschutzmitteilung) gegenüber dem VDA sowie der optionalen Angabe einer E-Mail-Adresse. Außerdem haben die E-ID-Werber*innen über das Vorregistrierungssystem auch einen Username und das Signaturpasswort festzulegen. Daraufhin wird durch das Vorregistrierungssystem ein QR-Code erzeugt, welcher den E-ID-Werber*innen auf der Website des VDA angezeigt wird. Die E-ID-Werber*innen haben daraufhin den QR-Code mit ihrer App „Digitales Amt“ zu scannen, wodurch es zur kryptographischen Bindung (Gerätebindung) bzw App-Verknüpfung zwischen der App „Digitales Amt“ (bzw ihrer VDA-Komponente) und der noch unvollständigen E-ID der E-ID-Werber*innen bzw der VDA-Domain kommt.

Um den gesamten E-ID-Registrierungsprozess erfolgreich abzuschließen, ist im Anschluss an den zuvor geschilderten Vorregistrierungsprozess der persönliche Besuch bei einer Registrierungsbehörde zur Durchführung der Identitätsfeststellung und Aktivierung der persönlichen ID Austria erforderlich.

Dabei ist zu beachten, dass die Vorregistrierung und der daran anschließende behördliche Teil des Registrierungsprozesses innerhalb von 30 Tagen erfolgen muss da sonst eine neue Vorregistrierung erforderlich ist oder eine andere Registrierungsvariante zur Anwendung gelangt. Nach der erfolgten Identifikation mittels Lichtbildausweis[124], rufen die zuständigen Behördenmitarbeiter*innen die Vorregistrierungsdaten der E-ID-Werber*innen auf und initiieren die finale Erstellung der ID Austria durch den VDA. Dabei erhalten die E-ID-Werber*innen eine TAN in ihre App „Digitales Amt“, die sie den Behördenmitarbeiter*innen mitzuteilen haben. Im Anschluss erfolgt die Erstellung der ID Austria, wodurch es zur kryptographischen Bindung zwischen der App „Digitales Amt“ (bzw ihrer VDA-Komponente) mit der VDA-Domain kommt; damit ist der gesamte E-ID- bzw ID Austria-Registrierungsprozess erfolgreich abgeschlossen und die persönliche ID Austria bzw E-ID ist in der betreffenden App aktiviert.

B. **Anmelden mit der Handy-Signatur in der App „Digitales Amt“**

Für diese Registrierungsvariante ist das Vorhandensein einer Handy-Signatur sowie die bereits auf dem Mobiltelefon der E-ID-Weber*innen installierten App „Digitales Amt“ erforderlich. Dabei fungiert das bestehende Handy-Signatur-Konto der E-ID-Werber*innen als eine Art Vorregistrierungssystem, da die Vorregistrierungsdaten bei dieser Registrierungsvariante von der Handy-Signatur bzw über den VDA bereitgestellt werden.

[124] Bei der Registrierungsvariante A sollte für die Identifikation und den erfolgreichen Abgleich mit den Vorregistrierungsdaten (bzgl angegebener Dokumentennummer) das bei der zuvor durchgeführten Vorregistrierung verwendete Dokument (Reisepass oder Personalausweis) verwendet werden. Ein entsprechender Hinweis wird im Rahmen der Vorregistrierung auf der Website des VDA bei der Auswahl dieser Registrierungsvariante erscheinen.

Zunächst ist die Anmeldung mittels bereits vorhandener Handy-Signatur in der App „Digitales Amt“ notwendig, denn dadurch sind die E-ID-Werber*innen für die Erstellung einer E-ID bzw einer ID Austria bereits vorregistriert. Auch in diesem Fall ist ein Zweitgerät erforderlich. In weiterer Folge müssen sich die E-ID-Werber*innen im Rahmen der persönlichen Identitätsfeststellung mittels einem gültigen Lichtbildausweises bei der Registrierungsbehörde eindeutig identifizieren lassen und bekannt geben, dass sie eine E-ID bzw ID Austria registrieren lassen möchten. Nach der erfolgten Identifikation rufen die jeweils zuständigen Behördenmitarbeiter*innen die Vorregistrierungsdaten der E-ID-Werber auf und initiieren die finale Erstellung der ID Austria durch den VDA; dabei wird die Versendung einer TAN durch den VDA ausgelöst. Daraufhin erhalten die E-ID-Werber eine TAN in ihre App „Digitales Amt“, die sie den Behördenmitarbeiter*innen mitzuteilen haben. Im Anschluss erfolgt die Erstellung der ID Austria, wodurch es zur kryptographischen Bindung zwischen der App „Digitales Amt“ (bzw ihrer VDA-Komponente) mit der VDA-Domain kommt; damit ist der gesamte E-ID- bzw ID Austria-Registrierungsprozess erfolgreich abgeschlossen und die persönliche ID Austria bzw E-ID ist in der betreffenden App aktiviert.

C. TAN aus der App „Digitales Amt“ ohne Handy-Signatur

Bei dieser Registrierungsvariante erscheinen die E-ID-Werber*innen ohne Vornahme spezifischer Vorbereitungsschritte (keine Vorregistrierung und keine vorhandene Handy-Signatur) bei der Registrierungsbehörde und starten dort den E-ID-Registrierungsprozess. Erforderlich hierfür ist lediglich das Vorhandensein der bereits auf dem Mobiltelefon der E-ID-Werber*innen installierten App „Digitales Amt“. So haben die E-ID-Werber*innen samt einem gültigen Lichtbildausweis zur persönlichen Identitätsfeststellung im Rahmen des E-ID-Registrierungsprozesses eine Registrierungsbehörde aufzusuchen. Von den Behördenmitarbeiter*innen erhalten die E-ID-Werber*innen einen ID Austria-Behördenausdruck auf dem sich ein Freischaltcode, Widerrufs-Passwort und QR-Code befinden. Die E-ID-Werber*innen öffnen die App „Digitales Amt“, scannen den auf dem betreffenden ID Austria-Behördenausdruck abgebildeten QR-Code ein und erhalten in die App „Digitales Amt“ eine TAN, welche die E-ID-Werber*innen der Behördenmitarbeiter*innen mitzuteilen haben. Die TAN wird daraufhin in das IDR eingetragen und der behördliche Teil dieser Registrierungsvariante ist damit abgeschlossen.

Der restliche Registrierungsprozess kann von zu Hause aus erfolgen, wofür ein Zweitgerät (zB Laptop) erforderlich ist. Dabei ist zu beachten, dass der nachfolgende Teil des Registrierungsprozesses innerhalb von drei Monaten nach dem Behördengang selbstständig abzuschließen ist, da sonst eine neue Registrierung samt behördlichem Teil erforderlich ist, oder eine andere Registrierungsvariante zur Anwendung gelangt. Hierbei ist zunächst das Smartphone mit der bereits darauf installierten App „Digitales Amt“ sowie der zuvor erhaltene ID Austria-Behördenausdruck bereitzustellen. Daraufhin haben die E-ID-Werber*innen mit ihrem Zweitgerät die Website des VDA zu öffnen und zu der Funktion, über die der E-ID-Registrierungsprozess abgeschlossen wurde, zu navigieren. Hierzu geben die E-ID-Werber*innen den auf dem ID Austria-Behördenausdruck befindlichen Freischaltcode und das Widerrufs-Passwort ein, übermitteln diese an den VDA und erteilen diesem gegenüber auch die hierfür erforderlichen Zustimmungen (Signaturvertrag, AGB, Datenschutzmitteilung). Daraufhin antwortet dieser den E-ID-Inhabern (bzw dessen Web-Browser am Zweitgerät) mit einem Web-Formular, über

das die E-ID-Inhaber einen Benutzernamen und ein Signaturpasswort zu definiert haben und sendet diese Daten wieder an den VDA. Anschließend generiert der VDA eine TAN und sendet diese an die App „Digitales Amt“ der E-ID-Werber*innen. Diese TAN haben die E-ID-Werber*innen mittels Anwendung der Funktion Fingerprint oder Face-ID zu bestätigen. Damit kommt es einerseits zur Erstellung eines VDA-Kontos, welches für die Funktion der Signaturerstellung notwendig ist und andererseits zur kryptographischen Bindung zwischen der App „Digitales Amt“ (bzw ihrer VDA-Komponente) mit der VDA-Domain. Dadurch sind der gesamte E-ID- bzw ID Austria-Registrierungsprozess erfolgreich abgeschlossen und die persönliche ID Austria bzw E-ID in der betreffenden App aktiviert.

D. **Registrierung mit SMS-TAN**

Für diese Registrierungsvariante sind zu Beginn weder das Vorhandensein der bereits installierten App „Digitales Amt“ noch der Besitz einer Handy-Signatur notwendig.

Zunächst ist zur persönlichen Identitätsfeststellung im Rahmen des E-ID-Registrierungsprozesses eine Registrierungsbehörde aufzusuchen. Von den Behördenmitarbeiter*innen erhalten die E-ID-Werber*innen einen ID Austria-Behördenausdruck, auf dem sich ein Freischaltcode und ein Widerrufs-Passwort befinden. Um im letzten Schritt die kryptographische Bindung zwischen der App „Digitales Amt“ der E-ID-Werber*innen (bzw ihrer VDA-Komponente) mit der VDA-Domain herzustellen, haben diese zunächst den Behördenmitarbeiter*innen ihre Mobiltelefonnummer zu deren Verifikation, die über SMS erfolgt, bekannt zu geben. Daraufhin erhalten die E-ID-Werber*innen eine SMS-TAN, die in Folge den Behördenmitarbeiter*innen mitzuteilen ist. Daraufhin ist der behördliche Teil dieser Registrierungsvariante abgeschlossen.

Der restliche Registrierungsprozess kann von zu Hause aus erfolgen, wofür ein Zweitgerät (zB Laptop) und von nun an auch die bereits auf dem Mobiltelefon der E-ID-Werber*innen installierte App „Digitales Amt“ erforderlich sind. Dabei ist zu beachten, dass der nachfolgende Teil des Registrierungsprozesses innerhalb von drei Monaten nach dem Behördengang selbstständig abzuschließen ist, da sonst eine neue Registrierung samt behördlichem Teil erforderlich ist oder eine andere Registrierungsvariante zur Anwendung kommt.

Für den restlichen Registrierungsprozess sind zunächst das Mobiltelefon mit der darauf bereits installierten App „Digitales Amt“ sowie der zuvor erhaltene ID Austria-Behördenausdruck bereitzustellen. Daraufhin haben die E-ID-Werber*innen mit ihrem Zweitgerät die Website des VDA zu öffnen und zur Funktion zu navigieren, über die ihr E-ID-Registrierungsprozess abgeschlossen werden kann. Hierzu geben die E-ID-Werber*innen den auf dem ID Austria-Behördenausdruck befindlichen Freischaltcode und das Widerrufs-Passwort ein, übermitteln diese an den VDA und erteilen diesem gegenüber auch die hierfür erforderlichen Zustimmungen (Signaturvertrag, AGB, Datenschutzmitteilung). Daraufhin antwortet dieser dem *E-ID-Inhaber* (bzw dem Web-Browser am Zweitgerät) mit einem Web-Formular, über das die *E-ID-Inhaber* einen Benutzernamen und ein Signaturpasswort zu definieren haben, und sendet diese Daten wieder an den VDA. Anschließend generiert der VDA eine SMS-TAN und sendet diese an die bereits von ihm verifizierte Telefonnummer der E-ID-Werber*innen. Diese geben dann die erhaltene SMS-TAN in ein Web-Formular auf dem

Zweitgerät ein und übermitteln dieses an den VDA. Letztendlich erhalten die E-ID-Werber*innen vom VDA über ihr Zweitgerät noch einen QR-Code, den sie mit ihrer App „Digitales Amt“ scannen. Durch diese Registrierungsvariante kommt es einerseits zur Erstellung eines VDA-Kontos, welches für die Funktion der Signaturerstellung notwendig ist, und andererseits zur kryptographischen Bindung zwischen der App „Digitales Amt“ (bzw ihrer VDA-Komponente) mit der VDA-Domain. Dadurch sind der gesamte E-ID- bzw ID Austria-Registrierungsprozess erfolgreich abgeschlossen und die persönliche ID Austria bzw E-ID in der betreffenden App aktiviert.

E. **Registrierung mit Post-TAN**

Für diese Registrierungsvariante sind zu Beginn weder das Vorhandensein der bereits installierten App „Digitales Amt“ noch der Besitz einer Handy-Signatur notwendig. Darüber hinaus bedarf es innerhalb des behördlichen Teils dieser Registrierungsvariante auch keines Mobiltelefons.

Zunächst ist zur persönlichen Identitätsfeststellung im Rahmen des E-ID-Registrierungsprozesses eine Registrierungsbehörde aufzusuchen. Dabei haben die E-ID-Werber*innen den Behördenmitarbeiter*innen auch eine Zustelladresse (Hauptwohnsitz oder beliebige Adresse) für die Zusendung der POST-TAN sowie optional ihre E-Mail-Adresse anzugeben. Von den Behördenmitarbeiter*innen erhalten die E-ID-Werber*innen einen ID Austria-Behördenausdruck, auf dem sich ein Freischaltcode und ein Widerrufs-Passwort befinden. Damit ist der behördliche Teil dieser Registrierungsvariante abgeschlossen.

Der restliche Registrierungsprozess, wofür ein Zweitgerät (zB Laptop) erforderlich ist, kann von zu Hause aus erfolgen und unterteilt sich in zwei aufeinanderfolgende Teilschritte. Dabei ist zu beachten, dass die nachfolgenden Teilschritte des Registrierungsprozesses innerhalb von drei Monaten nach dem Behördengang selbstständig abzuschließen sind, da sonst eine neue Registrierung samt behördlichem Teil erforderlich ist oder eine andere Registrierungsvariante zur Anwendung kommt.

Innerhalb des ersten Teilschritts wird die Mobiltelefonnummer der E-ID-Werber*innen verifiziert und diese legen einen Benutzer*innennamen und ein Passwort fest. Hierzu ist zunächst das Zweitgerät sowie der zuvor erhaltene ID Austria-Behördenausdruck bereitzustellen.

Daraufhin haben die E-ID-Werber*innen mit ihrem Zweitgerät die Website des VDA zu öffnen und zur Funktion zu navigieren, über die sie ihren E-ID-Registrierungsprozess abschließen können. Hierzu geben die E-ID-Werber*innen den auf dem ID Austria-Behördenausdruck befindlichen Freischaltcode und das Widerrufs-Passwort ein, übermitteln diese an den VDA und erteilen diesem gegenüber auch die hierfür erforderlichen Zustimmungen (Signaturvertrag, AGB, Datenschutzmitteilung). Daraufhin antwortet dieser den E-ID-Werber*innen (bzw deren Web-Browser am Zweitgerät) mit einem Web-Formular, in dem sie ihren Vornamen, Familiennamen, Geburtsdatum und Telefonnummer angeben und sendet diese Daten wieder an den VDA. Anschließend generiert der VDA eine SMS-TAN und sendet diese an die zuvor angegebene Telefonnummer der E-ID-Werber*innen. Im Anschluss daran erhalten die E-ID-Werber*innen per SMS eine TAN auf ihr Mobiltelefon, die sie auf der Website des VDA eingeben. Darauffolgend haben die E-ID-Werber*innen einen Benutzer*innennamen und ein Signaturpasswort auf der betreffenden Website zu definieren. Anschließend können sie zwischen dem Hauptwohnsitz und der bei der Behörde angegebenen Adresse für den Versand der Post-TAN per RSa-

Zustellung (persönliche Übergabe) wählen. Damit ist der erste Teilschritt dieser Registrierungsvariante von zu Hause aus beendet. Die E-ID-Werber*innen müssen nun auf den Erhalt der Post-TAN per RSa-Zustellung warten.

Innerhalb des zweiten Teilschritts, welcher erst nach Erhalt der Post-TAN erfolgen kann, schließen die E-ID-Werber*innen letztendlich den gesamten E-ID-Registrierungsprozess unter Verwendung der erhaltenen Post-TAN ab. Zunächst sind das Mobiltelefon mit der darauf bereits installierten App „Digitales Amt", ein Zweitgerät, die zuvor im ersten Teilschritt definierten Zugangsdaten (Benutzer*innenname und Signaturpasswort) sowie die bereits erhaltene Post-TAN bereitzustellen. Daraufhin haben die E-ID-Werber*innen mit ihrem Zweitgerät die Website des VDA zu öffnen und sich dort für den Abschluss des Registrierungsprozesses mit den zuvor definierten Zugangsdaten und der Post-TAN anzumelden bzw sich gegenüber dem VDA damit zu authentifizieren. Im Anschluss daran erhalten die E-ID-Werber*innen per SMS eine TAN auf die Mobiltelefonnummer, die sie auf der Website des VDA eingeben. Nun ist die App „Digitales Amt" mit dem Mobiltelefon zu öffnen, um damit den QR-Code, der den E-ID-Werber*innen auf ihrem Zweitgerät via VDA-Website angezeigt wird, zu scannen. Durch diese Registrierungsvariante kommt es einerseits zur Erstellung eines VDA-Kontos, welches für die Funktion der Signaturerstellung notwendig ist und andererseits zur kryptographischen Bindung zwischen der App „Digitales Amt" (bzw ihrer VDA-Komponente) mit der VDA-Domain. Dadurch sind der gesamte E-ID- bzw ID Austria-Registrierungsprozess erfolgreich abgeschlossen und die persönliche ID Austria bzw E-ID in der betreffenden App aktiviert.

F. **Vereinfachter Umstieg**

Um einen reibungslosen Übergang auf das neue E-ID-System zu gewährleisten, wird Inhaber*innen einer Bürgerkarte (Handy-Signatur) ermöglicht werden, vereinfacht auf einen E-ID umzusteigen, mit dem sie sämtliche neue Funktionen nutzen können, wie zB den Nachweis der Lenkberechtigung gem § 15a des Führerscheingesetzes (FSG),[125] und in weiterer Folge auch den Nachweis von personenbezogenen Daten gem § 18 Abs 1 E-GovG. Zum Zeitpunkt der Erstellung des vorliegenden Berichts befindet sich die konkretisierende Regelung in Verordnungsform noch im Prozess vor der Erlassung der VO. Diese VO stützt sich auf die Verordnungsermächtigung in § 25 Abs. 3 letzter Satz E-GovG.

Wie nachfolgend ausgeführt wird, soll in bestimmten Fällen der ansonsten erforderliche Registrierungsprozess gem § 4a Abs. 1 E-GovG entfallen, da bereits eine gleichwertige behördliche Identitätsüberprüfung im Zuge der Ausstellung der Funktion Bürgerkarte stattgefunden hat. Voraussetzung für den vereinfachten Umstieg auf den E-ID mit vollem Funktionsumfang ist, dass die betreffende Bür-gerkarte durch ein oberstes Organ des Bundes oder der Länder, einen Bürgermeister, eine Bezirksver-waltungsbehörde oder das Finanzamt Österreich – insbesondere auch auf elektronischem Weg über FinanzOnline – ausgestellt wurde. Darüber hinaus bedarf es für den vereinfachten Umstieg eines gül-tigen österreichischen Reisepasses (ausgenommen eines Notpasses gem § 4a des Passgesetzes 1992) oder gültigen österreichischen Personalausweises des Inhabers der Bürgerkarte, damit die Person einem bestehenden Eintrag in der Datenverarbeitung gem § 22b des

[125] Siehe Bundesgesetz über den Führerschein (Führerscheingesetz – FSG), StF: BGBl. I Nr. 120/1997.

Passgesetzes 1992 (IDR) zugeordnet werden kann. Von der gewählten Formulierung sind hingegen weder Fremden- und Konventionspässe noch ausländische Reisedokumente umfasst.

Schließlich soll im Rahmen des vereinfachten Umstiegs auf den neuen E-ID sichergestellt werden, dass durch die/den E-ID-Werber*in keine entfremdeten Identitätsdokumente vorgelegt werden. Eine Abfrage im Rahmen der Sachenfahndung – einer Datenverarbeitung einer Sicherheitsbehörde – dient der Überprüfung der Identität und der vorgelegten Dokumente, wie dies in § 4a Abs. 4 dritter Satz E-GovG vorgesehen ist. Sofern die Voraussetzungen gemäß Z 1 bis 3 nicht vorliegen, ist der Umstieg auf einen E-ID mit sämtlichen Funktionen nur vor Ort bei einer Registrierungsbehörde gemäß § 4a Abs 1 oder 2 E-GovG möglich. Der vereinfachte Umstieg auf einen E-ID hat keine Auswirkungen auf die verbleibende Gültigkeitsdauer der bisherigen Bürgerkarte bzw des bereits ausgestellten qualifizierten Zertifikats. Eine selbständige Verlängerung des E-ID beim VDA unter Verwendung der Funktion E-ID soll ermöglicht werden.

Damit bereits ausgestellte Bürgerkarten mit Start des Echtbetriebs möglichst einfach in das neue technische System übergeführt werden können, soll unabhängig von der oben dargestellten Lösung die Möglichkeit bestehen, unter Beibehaltung des bisherigen Funktionsumfangs auf einen E-ID umzusteigen (E-ID mit Basisfunktion). Darüber hinaus hat der vereinfachte Umstieg auch keine Auswirkung auf die verbleibende Gültigkeitsdauer der bisherigen Bürgerkarte bzw des bereits ausgestellten qualifi-zierten Zertifikats. Betroffenen, die auf einen E-ID mit Basisfunktion umgestiegen sind, soll es selbst-verständlich freistehen, den behördlichen Registrierungsprozess gemäß § 4a E-GovG – sowohl vor als auch nach Ablauf der Gültigkeitsdauer des E-ID – abzuschließen, um von sämtlichen Funktionen des E-ID zu profitieren.

3.2.3 Verwendung der ID Austria

Haben die Bürger*innen den Registrierungsprozess erfolgreich durchlaufen, steht ihnen die ID Austria zur Verwendung zur Verfügung. Dabei kann die ID Austria zur Erstellung einer qualifizierten elektronischen Signatur (diese ist rechtlich der handschriftlichen Unterschrift weitgehend gleichgestellt), zur Erstellung eines Bindings an die ID Austria (zur vereinfachten Weiterverwendung einer Authentifizierung am ID Austria System), sowie zur Anmeldung an einem Service Provider (als Single-Sign-On-Dienst iSe zentralen Login-Funktion) verwendet werden. Die Anwendungsfälle der ID Austria werden nachfolgend näher beschrieben.

3.2.3.1 Erstellung einer qualifizierten elektronischen Signatur

Nach Durchführung des Registrierungsprozesses können die Benutzer*innen (als *ID Austria-Inhaber* bzw *E-ID-Inhaber*) die ID Austria bzw das damit verknüpfte Zertifikat zur Erstellung einer qualifizierten Signatur (zB PDF-Signatur) verwenden.

Das dafür nötige qualifizierte Zertifikat (bzw der mit diesem Zertifikat verknüpfte private Signaturschlüssel) wird zentral durch den VDA verwaltet. Zur Erstellung einer qualifizierten Signatur authentifizieren sich die Benutzer*innen mit den für ihre ID Austria registrierten Authentifizierungsfaktoren beim VDA (bspw User-ID/Passwort als Wissensfaktor und Mobiltelefon als Besitzfaktor), woraufhin dieser die Signatur für die jeweiligen Benutzer*innen erstellt.

Die Erstellung einer qualifizierten Signatur kann sowohl in einem Web-Browser als auch in mobilen Apps gestartet werden. Der Signaturprozess kann über die Client-Komponente („Digitales Amt“-App, eine Third-Party-App, einen Web-Browser) initiiert werden. Bei Verwendung jeder Client-Komponente sind unterschiedliche Möglichkeiten zur Erstellung und Übermittlung einer Signatur gegeben. Konkret sind folgende Varianten der Signaturerstellung und -übermittlung möglich:

- **Signaturerstellung direkt über die Client-Komponente:** Die verwendete mobile Applikation erstellt selbstständig einen Signaturerstellungs-Request (sozusagen eine Anfrage) und übermittelt diesen direkt an den VDA. Mit dem erfolgreichen Authentifizierungsprozess wird die beim VDA erstellte Signatur direkt an die Client-Komponente retourniert.

- **Signaturerstellung über einen serverseitigen Service Provider:** Die verwendete Client-Komponente dient diesfalls nur als User-Interface für einen serverseitigen SP (vergleichbar mit einem Webserver). Der Signaturerstellungsprozess wird durch eine Interaktion der Benutzer*innen mit der Client-Komponenten ausgelöst. Der Signaturerstellungs-Request wird jedoch vom SP erstellt und von dort an den VDA übermittelt. Nach erfolgter Benutzer*innenauthentifizierung über die jeweilige Client-Komponente wird die erstellte Signatur an den serverseitigen SP zurückgesendet.

- **Signaturerstellung über die „Digitales Amt“-App:** Für diese Variante bietet die „Digitales Amt“-App eine lokale Signaturerstellungs-Schnittstelle an. Client-Komponenten (hier zumeist Apps), die sich am gleichen Gerät wie die „Digitales Amt“-App befinden, können Signatur-Requests lokal am

Endgerät an diese Schnittstelle schicken. Zur Erstellung der qualifizierten Signatur übermittelt die „Digitales Amt“-App einen entsprechenden Signaturerstellungs-Request an den VDA. Die erstellte Signatur wird vom VDA zunächst an die „Digitales Amt“-App zurückgesendet, welche die Signatur über die lokale Schnittstelle dann an die entsprechende Client-Komponente, die jenen Prozess aufgerufen hat, weiterleitet. Zu beachten gilt es hierbei, dass die „Digitales Amt“-App diesfalls nicht die Client-Komponente darstellen kann.

3.2.3.2 Binding-Erstellung

Nach erfolgreicher Registrierung steht den Benutzer*innen auch die Option einer Binding-Erstellung offen. Damit können Benutzer*innen ihr mobiles Gerät unter Verwendung der „Digitales Amt“-App kryptographisch an den Identity Provider[126] des ID Austria Systems binden. Mit dieser Bindung kann in weiterer Folge eine vereinfachte Authentifizierung gegenüber diesem Identity Provider erfolgen, wobei der Identity Provider der ID Austria[127] die Funktion des VDA[128] übernimmt.[129]

Die Erstellung der Bindung wird unter Verwendung der VDA-Komponente[130] der „Digitales Amt“-App durchgeführt. Dazu kontaktiert die ID Austria-Komponente der „Digitales Amt“-App den Bindungsservice des Identity Providers, der Informationen zur Erstellung eines Schlüsselpaares (Public/Private Key) an die ID Austria-Komponente zurücksendet. Die Erstellung von Schlüsselmaterial in Smartphones wird durch spezielle Hardware-Elemente ermöglicht, die eine sichere Schlüsselerzeugung und -speicherung gewährleisten. Die Verwendung des Schlüsselmaterials im Smartphone wird lokal durch eine Authentifizierungsmethode geschützt. Im Falle der „Digitales Amt“-App kommen hierbei Fingerprint bzw FaceID zum Einsatz.

Nach erfolgreicher Nutzer*innenauthentifizierung wird das Bindungszertifikat ausgestellt, welches schließlich im User Store[131] des ID Austria Systems eingetragen und zur ID Austria-Komponente der „Digitales Amt“-App der Benutzer*innen zurückgeschickt wird. Hiernach ist das Bindungszertifikat am ID Austria System registriert und kann zusammen mit dem zugehörigen privaten Schlüssel, der sicher am Smartphone der jeweiligen Benutzer*innen gespeichert ist, für die vereinfachte Weiterverwendung dieser vorherigen Authentifizierung verwendet werden.

Bei einem derartigen, aufrechten Binding erschöpft sich die erforderliche Nutzer*inneninteraktion im Rahmen des Authentifizierungsvorgangs auf die biometrische Authentifizierung am mobilen Gerät, obwohl nach wie vor zwei Authentifizierungsfaktoren zur Anwendung kommen.[132]

---

[126] Die Funktion des Shibboleth Identity Providers als zentraler Identity Provider des ID Austria Systems besteht darin, die Authentifizierung des *E-ID-Inhabers* und die Zusammenführung aller notwendigen Identitätsattribute (siehe zu diesen etwa bereits 3.1) zu gewährleisten, wobei er diese Aufgaben an andere Komponenten des Systems überträgt.
[127] Im Folgenden kurz „Identity Provider“.
[128] Siehe zu dieser schon grundlegend 3.1.
[129] Die VDA-Funktion der qualifizierten Signatur wird jedoch nicht übernommen.
[130] Siehe zu dieser 3.1 (User Domain).
[131] Im User Store werden relevante Informationen zu den *ID Austria-Inhabern*, wie diesfalls etwa Informationen zur kryptografischen Bindung, gespeichert. Dieser ist Teil der E-ID-Frontend-Domain (siehe zu dieser 3.1). Der Idenity Provider hat hierauf Zugriff und kann dadurch die vereinfachte Authentifizierung durchführen.
[132] Faktor Besitz: kryptographisches Schlüsselmaterial bzw. jene Hardware, die dieses Schlüsselmaterial enthält; Faktor Biometrie: Fingerprint bzw Face-ID.

Ein Service Provider kann im Zuge seiner Registrierung/Akkreditierung[133] die Unterstützung der eben beschriebenen vereinfachten Authentifizierung beeinflussen, wobei dies über verschiedene Parameter geschehen kann. Im Extremfall kann der Einsatz dieser vereinfachten Weiterverwendung einer vorherigen Authentifizierung ganz ausgeschlossen und die Benutzer*innen stets zur Durchführung VDA-basierter Authentifizierungsprozesse[134] gezwungen werden.

3.2.3.3 Anmeldung an Service Provider

Aus Sicht des *Inhabers* einer ID Austria stellt die Anmeldung an Service Providern neben Signaturerstellungsprozessen den Hauptanwendungsfall des ID Austria Systems dar. Nach erfolgter Registrierung und der soeben beschriebenen optionalen Binding-Erstellung kann eine Anmeldung an Service Providern beliebig oft wiederholt werden, solange die ID Austria gültig ist.

Service Owner können die Funktionsweise des Logins bzw. der Anmeldung von Benutzer*innen an ihre Service Provider, wie etwa Web-Applikationen oder Apps damit an die ID Austria auslagern. Die ID Austria übernimmt dabei dementsprechend die Rolle eines Identity Providers.

Im Folgenden werden, die im Zuge einer Authentifizierung anfallenden Verarbeitungsvorgänge beschrieben. Basis aller dabei beschriebenen Protokolle und Varianten ist die Kommunikation zwischen der „Digitales Amt"-App, dem Service Provider und dem zentralen Identity Provider des ID Austria Systems.

Diese Kommunikation erfolgt über die Protokolle SAML 2.0 bzw Open ID Connect (OIDC). OIDC hat sich speziell im mobilen Umfeld als präferierter Standard zur Umsetzung von Identitätsmanagementsystemen und für die Interaktion zwischen Service Providern und Identity Providern etabliert. Dementsprechend unterstützt auch die ID Austria OIDC zur Interaktion mit (mobilen) Service Providern. SAML 2.0 wird hauptsächlich bei der Authentifizierung im Rahmen von Web-Applikationen verwendet.

Die im Rahmen der Authentifizierung über die Protokolle SAML 2.0 bzw OIDC stattfindenden Datenflüsse stellen sich wie folgt dar:

SAML 2.0:

1. Der Service Provider erstellt einen SAML 2.0 Authentifizierungs-Request (also quasi eine Anfrage), welcher den Benutzer*innen übermittelt wird.
2. Die Benutzer*innen senden diesen Authentifizierungs-Request an den Identity Provider des ID Austria Systems.
3. Dieser übermittelt eine Auswahl der zur Verfügung stehenden Authentifizierungsmethoden an den Web-Browser der Benutzer*innen für die entsprechende Weiterleitung. Die Authentifizierung erfolgt bei der Verwendung einer registrierten, persönlichen ID Austria über den *Vertrauensdienstanbieter* (VDA, VDA-AUTH), das eIDAS System, die Statistik Austria-Domain, die SZRB-Domain und die USP/PVP-Domain. Soweit ein Binding an den Identity Provider

[133] Siehe hierzu 3.2.1.
[134] Siehe zu diesen bereits oben.

des ID Austria Systems erstellt wurde, findet die Authentifizierung dort statt (BINDING-AUTH). Soweit während der Authentifizierung biometrische Daten verarbeitet werden, geschieht dies ausschließlich lokal am Endgerät.

4. Nach erfolgreicher Benutzer*innenauthentifizierung erstellt die ID Austria eine sogenannte SAML2-Assertion, dh eine signierte Datenstruktur, die u.a. die Attribute der Benutzer*innen enthalten kann. Diese SAML2-Assertion wird von der ID Austria verschlüsselt über eine Authentifizierungs-Response (also quasi als Antwort) an die Benutzer*innen übermittelt. Bei Auslieferung von anderen Attributen als Name und Geburtsdatum (Minimal Dataset) wird die datenschutzrechtliche Einwilligung der Benutzer*innen eingeholt.[135]
5. Die Benutzer*innen senden die so erhaltene SAML 2.0 Authentifizierungs-Response mittels eines sogenannten HTTP-POST-Requests an den Service Provider. Dabei handelt es sich um eine Anfrage durch das im Webbereich für synchrone Kommunikation zwischen Server und Endnutzer*innengerät verwendete Hypertext Transfer Protocol.[136] „POST" bezeichnet in diesem Zusammenhang die Methode dieser Kommunikation.
6. Der Service Provider kann aus einem Teil der erhaltenen SAML 2.0 Authentifizierungs-Response (nämlich der SAML2-Assertion), die von der ID Austria bestätigten Daten (Attribute) der Benutzer*innen entnehmen und diese so der entsprechenden Anwendung übergeben.

Open ID Connect (OIDC):

1. Der entsprechende Service Provider erstellt einen OIDC Authentifizierungs-Request (also wiederum eine Anfrage), welcher den Benutzer*innen übermittelt wird.
2. Die Benutzer*innen senden den Authentifizierungs-Request an den Identity Provider (IDP) des ID Austria Systems.
3. Der IDP übermittelt eine Auswahl der zur Verfügung stehenden Authentifizierungsmethoden an den Web-Browser zur entsprechenden Weiterleitung. Die Authentifizierungsoptionen gleichen jenen bei SAML 2.0 (siehe Datenfluss SAML 2.0 - Punkt 3). Bei Auslieferung anderer Attribute als Name und Geburtsdatum (Minimal Dataset) wird die datenschutzrechtliche Einwilligung der Benutzer*innen eingeholt.[137]
4. Nach erfolgreicher Benutzer*innenauthentifizierung antwortet der IDP den Benutzer*innen wiederum mit einer Authentifizierungs-Response, die den Authorization-Code beinhaltet.
5. Der erhaltene Authorization-Code wird dabei vom Endgerät der Benutzer*innen an den Service Provider übermittelt.
6. Der Service Provider sendet den Authorization-Code in einem sogenannten Token-Request an den Token-Endpoint, also eine entsprechende Schnittstelle, der ID Austria.
7. Nach erfolgreicher Validierung des Authorization-Codes durch die ID Austria antwortet diese mit einer OIDC-Successful-Token-Response, also einer Antwort, die das signierte und verschlüsselte ID-Token enthält. Dieses ID-Token liefert die angeforderten Attribute (Claims) sowie die Signatur

[135] Die Auslieferung von weiteren persönlichen Attributen an Service Provider soll aus zugänglichen Datenquellen (wie zB aus öffentlichen Verwaltungsregistern) und ausschließlich nach Zustimmung der Benutzer*innen erfolgen; vgl *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper - Hintergrundinformationen (2021) 9, 14.
[136] Vgl *Ackermann*, Javascript - Das umfassende Handbuch² (2020) 505.
[137] Vgl *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 9, 14.

des Identity Providers in Form einer auf dem JSON-Standard basierenden Datenstruktur[138] an den Service Provider.

8. Der SP kann das erhaltene ID-Token schließlich entschlüsseln und dekodieren und mit den darin enthaltenen Attributen die Benutzer*innen in der Anwendung anmelden.

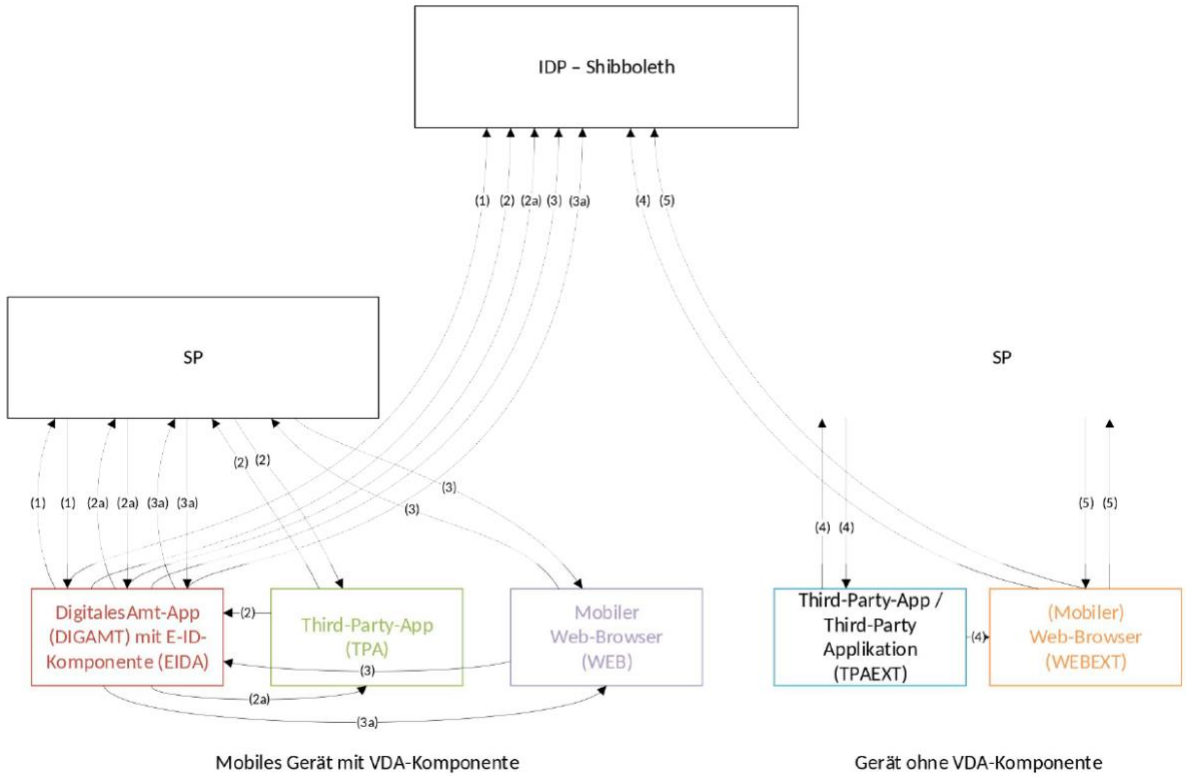

Abbildung 2: Varianten der Anmeldung an einem Service Provider bei Verwendung unterschiedlicher Client-Komponenten (siehe sogleich unten die Varianten 1 bis 5)

Abhängig davon, aus welcher Anwendung bzw von welchem Gerät sich die Benutzer*innen anmelden, sind den oben beschriebenen Protokollen SAML 2.0 und OIDC spezifische Kommunikationen vor- bzw nachgelagert.

Variante 1: Anmeldung aus „Digitales Amt"-App mit Anmeldeziel Service Provider

Die Benutzer*innen befinden sich in der „Digitales Amt"-App. Die App greift auf einen Service Provider (SP) zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der über die „Digitales Amt"-App an den Identity Provider der ID Austria übermittelt wird. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die *E-ID-Inhaber* werden aus der E-ID-Komponente zurück in die „Digitales Amt"-App weitergeleitet.

[138] JSON steht für *JavaScript Object Notation* und bezeichnet ein gängiges Format für den Austausch von Daten etwa zwischen Server und Endnutzer*innengerät: vgl hierzu *Ackermann*, Javascript[2] 510 f, 516.

Variante 2: Anmeldung aus Third-Party-App mit Anmeldeziel Third-Party-App
Die Benutzer*innen befinden sich in einer Third-Party-App (also einer mobilen Applikation eines Drittanbieters), die sich am gleichen Gerät wie die „Digitales Amt“-App befindet. Diese Third-Party-App greift auf einen Service Provider (SP) zu. Dieser SP erstellt daraufhin einen Authentifizierungs-Request, der zunächst über die entsprechende Third-Party-App an die „Digitales Amt“-App und von dort weiter an den Identity Provider des ID Austria Systems (IDP) übermittelt wird. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den entsprechenden SP. Die Nutzer*innen werden in die entsprechende Third-Party-App geleitet.

Variante 2a: Anmeldung aus „Digitales Amt“-App mit Anmeldeziel Third-Party-App
Die Benutzer*innen befinden sich beim Start des Anmeldeprozesses in der „Digitales Amt“-App. Diese greift auf den Service Provider (SP) zu, welcher daraufhin einen Authentifizierungs-Request erstellt, der über die „Digitales Amt“-App an den Identitätsprovider des ID Austria Systems (IDP) übermittelt wird. Die Benutzer*innenauthentifizierung durch den IDP erfolgt über die „Digitales Amt“-App. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den entsprechenden SP. Die Benutzer*innen werden aus der ID Austria-Komponente der „Digitales Amt“-App in die entsprechende Third-Party-App weitergeleitet. Dabei wird auch jene notwendige Information an die Third-Party-App übergeben, über welche die authentifizierte Sitzung zwischen dieser App und dem SP hergestellt werden kann.

Variante 3: Anmeldung aus mobilem Webbrowser mit Anmeldeziel mobiler Webbrowser
Die Benutzer*innen befinden sich in einem mobilen Web-Browser, der sich am gleichen Gerät wie die „Digitales Amt“-App mit ID Austria-Komponente befindet. Dieser Browser greift auf einen Service Provider (SP) zu. Jener SP erstellt daraufhin einen Authentifizierungs-Request, der zunächst über den entsprechenden mobilen Browser an die ID Austria-Komponente der „Digitales Amt“-App und von dort an den Identity Provider der ID Austria (IDP) übermittelt wird. Die Benutzer*innenauthentifizierung durch den IDP erfolgt über die ID Austria-Komponente der „Digitale -Amt“-App. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*innen werden aus der ID Austria-Komponente in den entsprechenden mobilen Browser zurückgeleitet.

Variante 3a: Anmeldung aus „Digitales Amt“-App mit Anmeldeziel mobiler Webbrowser
Die Benutzer*innen befinden sich beim Start des Anmeldeprozesses in der „Digitales Amt“-App. Dementsprechend greift die „Digitales Amt“-App auf einen Service Provider (SP) zu. Jener SP erstellt daraufhin einen Authentifizierungs-Request, der über die „Digitales Amt“-App und ihre ID Austria-Komponente an den Identity Provider des ID Austria Systems (IDP) übermittelt wird. Die Benutzer*innenauthentifizierung durch den IDP erfolgt über die „Digitales Amt“-App. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den entsprechenden SP. Die Benutzer*innen werden aus der ID Austria-Komponente in den entsprechenden Browser weitergeleitet. Dabei wird auch jene notwendige Information an diesen Browser übergeben, über welche die authentifizierte Sitzung zwischen jenem Browser und dem entsprechenden SP etabliert werden kann.

Variante 4: Anmeldung aus Zweitgerät mit Anmeldeziel Third-Party-App
Die Benutzer*innen befinden sich in einer Third-Party-App, die sich auf einem anderen Gerät als die „Digitales Amt"-App befindet. Diese Third-Party-App greift auf einen Service Providers (SP) zu. Dieser SP erstellt daraufhin einen Authentifizierungs-Request, der an die entsprechende Third-Party-App zurückgeschickt wird. Sofern in jener Third-Party-App eine Web-View-Komponente implementiert ist, wird der Authentifizierungs-Request von dieser App selbst an den IDP (über einen Redirect) übermittelt. Ansonsten nutzt die entsprechende App einen Web-Browser am selben Gerät, um den Authentifizierungs-Request an den IDP zu übermitteln. Die Authentifizierung erfolgt dementsprechend entweder in der entsprechenden Third-Party-App oder im angesprochenen Web-Browser. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den entsprechenden SP. Gegebenenfalls werden die Benutzer*innen aus dem Browser in die entsprechende Third-Party-App zurückgeleitet.

Variante 5: Anmeldung auf Zweitgerät mit Anmeldeziel Webbrowser
Die Benutzer*innen befinden sich in einem Web-Browser, der sich auf einem anderen Gerät als die „Digitales Amt"-App befindet. Der Browser greift auf einen Service Providers (SP) zu. Jener SP erstellt daraufhin einen Authentifizierungs-Request, der an den entsprechenden Browser zurückgeschickt und von dort an den Identity Provider des ID Austria Systems (IDP) übermittelt wird. Die Authentifizierung erfolgt im angesprochenen Web-Browser unter Verwendung eines zweiten Faktors. Nach erfolgter Authentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den entsprechenden SP. Die Benutzer*innen verbleiben während des gesamten Prozesses im Web-Browser.

Folgende Daten werden verarbeitet:

- Vorname, Nachname, Geburtsdatum (im Fall von öffentlichen Service Provider)
- Attribute (soweit zusätzliche Attribute über den Minimaldatensatz freigegeben werden)
- Biometrische Daten (Fingerabdruck und Gesichtsprofil) werden nicht an die SZRB übermittelt; sie verlassen das lokal im Benutzer*innen-Endgerät angesiedelte Secure Element nicht.[139]
- bcBind inkl. vSZ (verschlüsselte Stammzahl) der Betroffenen
- Qualifiziertes Signaturzertifikat der Benutzer*innen
- Signierten Auth-Block
- Device Infos (Allgemeine Betriebssysteminformationen)
- Signatur der Benutzer*innen
- Zusätzliche Informationen zur Authentifizierung (LoA, Timestamp, etc)
- Transaktions-ID – Eindeutiger Identifikator der Transaktion
- Datum und Zeit der Transaktion
- bPK (bereichsspezifisches Personenkennzeichen) der Betroffenen

[139] Eine Verarbeitung dieser Daten durch die Stammzahlenregisterbehörde im Rahmen des E-ID Systems erfolgt zu keinem Zeitpunkt. Biometrische Daten werden zu keinem Zeitpunkt im Rahmen der Registrierung gespeichert und sind ausschließlich am Gerät zu finden. Deswegen ist das BMDW nicht *Verantwortlicher* bezüglich dieser Verarbeitung. Es wird hier nur eine Funktion des Betriebssystems genutzt, wie dies auch zahlreiche andere Apps machen.

- Liste der übermittelten Attribute (ohne die konkreten Attributwerte)
- Service Provider-ID
- Daten, die für die technische Funktion notwendig sind (zB Bindung-Zertifikat, App-ID, Signaturzertifikat)
- Zeitstempel der letzten Verwendung
- Konfigurationseinstellungen der Benutzer*innen (zB Einwilligungen der Benutzer*innen)
- Vollmachteninfos (sofern vorhanden)

3.2.4 Verwaltung des E-ID über „Meine ID Austria“

Im Fall der Funktion „Meine ID Austria“ handelt es sich um Verarbeitungen, welche es Nutzer*innen erlauben, ihre ID Austria zu verwalten. Sie sind als Funktion in der „Digitales Amt“-App und in Form einer Website[140] umgesetzt. Die App ist im App Store von Google und Apple kostenlos via Download erhältlich.[141] Einzelne Verwaltungshandlungen sind persönlich bei der zuständigen Stelle einzubringen. Die Authentifizierung gegenüber der ID Austria wird mittels Anmeldevorgang (siehe oben) durchgeführt.

Push Nachrichten (Notifications) durch die „Digitales Amt“-App werden über Firebase Cloud Messaging[142] (FCM) versendet. Bei der Verwendung von iOS erfolgt der Versand zusätzlich über das Apple Push Notification Service (APNs)[143]. Dabei ist die Option, Google Analytics zu verwenden, deaktiviert. Damit die Nachrichten an die jeweiligen Adressat*innen verschickt werden können, wird eine nicht personenbezogene ID für die App generiert und in FCM – bei iOS zusätzlich in APNs – sowie im Push Notification Service der App verarbeitet. Um die Funktion Push Nachrichten benutzen zu können, müssen Benutzer*innen dies der App erlauben. Dazu öffnet die App einen Betriebssystem-Dialog nachdem die Nutzungsbedingungen akzeptiert wurden. In den Systemeinstellungen können die Benutzer*innen ihre Auswahl jederzeit ändern, wobei für die Wirksamkeit der Änderung jedoch in die App zurück gewechselt werden muss.

Die Website und die App nutzen das Open-Source-Tool Matomo um Zugriffsstatistiken zu generieren. Dazu werden die Log-Daten in das Tool Matomo geladen und dabei anonymisiert. Mit Matomo werden keine Daten an Server übermittelt, die außerhalb der Kontrolle des BMDW liegen.

„Meine ID Austria“ ist die zentrale Verwaltungsstelle der Benutzer*innen und bietet neben ihrer Funktion als Nutzer*innen-Komponente während der Verarbeitungen „Registrierung der Benutzer*innen“ sowie „Verwendung der ID Austria“ auch die nachfolgend aufgelisteten Funktionen. Den eIDAS-Benutzer*innen stehen innerhalb der Applikation nur die „Einsicht in Transaktions-Logs“ sowie der Widerruf offen.

---

[140] Siehe https://www.oesterreich.gv.at/id-austria.html (abgerufen am 22. 04. 2022).
[141] Bei Android im Google Play Store unter https://play.google.com/store/apps/details?id=at.gv.oe.app&hl=de_AT&gl=US (abgerufen am 22. 04. 2022); im Apple App-Store unter https://apps.apple.com/at/app/digitales-amt/id1454775189 (abgerufen am 22. 04. 2022).
[142] Lösung für das Versenden von Push-Nachrichten auf Android-Geräten; vgl https://firebase.google.com/docs/cloud-messaging (abgerufen am 22. 04. 2022).
[143] Lösung für das Versenden von Push-Nachrichten auf Apple-Geräten, vgl https://developer.apple.com/go/?id=push-notifications (abgerufen am 22. 04. 2022).

Einsicht in Transaktions-Logs:
Über diesen Prozess können die Benutzer*innen Einsicht in ihre persönlichen (und serverseitig gespeicherten) Transaktions-Logdaten nehmen. Auf diese Weise können die Benutzer*innen zum Beispiel ihre letzten Verwendungen (Authentifizierungsprozesse, Signaturprozesse) nachvollziehen.

Erneuerung der ID Austria:
Über diesen Prozess können die Benutzer*innen ihr qualifiziertes Signaturzertifikat erneuern und damit die Gültigkeit ihrer ID Austria verlängern lassen.

Registrierung zusätzlicher Authentifizierungsfaktoren:
Über diesen Prozess können die Benutzer*innen für ihre bestehende ID Austria zusätzliche Authentifizierungsfaktoren registrieren. Diese Funktion ist derzeit nicht umgesetzt.

Widerruf:
Über diese Prozesse können die Benutzer*innen folgende Elemente widerrufen:

- Qualifiziertes Zertifikat
- VDA-Binding zwischen dem VDA und der ID Austria-Komponente innerhalb der "Digitales Amts"-App
- ID Austria-Binding zwischen dem Identity Provider des ID Austria Systems und der ID Austria-Komponente innerhalb der „Digitales Amt"-App

Der Widerruf eines Elements kann den automatischen Widerruf anderer Elemente nach sich ziehen.

Folgende Varianten bestehen, einen Widerruf zu initiieren:

Widerruf des qualifizierten Zertifikats: Die Benutzer*innen initiieren den Widerruf ihres qualifizierten Zertifikats bei der Passbehörde oder beim VDA. Dies führt implizit auch zum Widerruf sämtlicher Bindings (VDA-Binding und ID Austria-Binding), die über dieses Zertifikat ausgestellt wurden. Die Benutzer*innen müssen nach Inanspruchnahme dieser Widerrufsoption erneut den Registrierungsprozess durchlaufen.

Widerruf durch Abmeldung: Die Benutzer*innen initiieren in ihrer „Digitales Amt"-App über die Funktion „Alle Geräte Abmelden" eine Deaktivierung der App, einen Widerruf des VDA-Bindings innerhalb der VDA-Komponente oder deaktivieren über ihre „Digitales Amt"-App oder das "Meine ID Austria" Webinterface gezielt ausgewählte oder alle Instanzen ihrer „Digitales Amt"-App. Dabei wird das bestehende VDA- Binding und in weiterer Folge auch ein bestehendes ID Austria-Binding widerrufen. Das qualifizierte Zertifikat der Benutzer*innen bleibt gültig. Verfügen die Benutzer*innen nach Abschluss dieses Prozesses über eine weitere „Digitales Amt"-App mit einsatzbereiter VDA-Komponente auf einem anderen Gerät, können diese ihre ID Austria wie gewohnt weiterverwenden. Ist keine weitere aktivierte/gebundene „Digitales Amt"-App mit VDA-Komponente für die Benutzer*innen verfügbar, müssen diese einen Recovery-Prozess durchlaufen, um wieder zu einer

einsatzbereiten App zu gelangen. Ist die Durchführung des Recovery-Prozesses nicht möglich, müssen die Benutzer*innen den Registrierungsprozess erneut durchlaufen.

Widerruf aufgrund eines gerooteten Endgerätes: Die VDA-Komponente in der „Digitales Amt"-App erkennt ein Rooting des mobilen Geräts und initiiert daraufhin den Widerruf des bestehenden VDA-Bindings zwischen dem VDA und dem betroffenen Gerät. Dazu sendet die VDA-Komponente einen entsprechenden Request an den VDA. Nach erfolgtem Widerruf der VDA-Bindung informiert der VDA das Widerrufs-Service, welches daraufhin ein eventuell bestehendes ID Austria-Bindungszertifikat zum betroffenen Gerät widerruft.

Folgende Daten werden verarbeitet:

- Vornamen
- Nachname
- Geschlecht
- Geburtsdatum
- Staatsangehörigkeit
- ID Austria-Binding-Zertifikat
- bPK
- IP-Adresse der Anfragenden
- Aufrufmethode (GET, HEAD, PUT)
- Zieladresse ohne HOST
- Protokoll mit Version (zB HTTP/1.1)
- Name der abgerufenen Serverdatei und übertragene Datenmenge
- Datum und Uhrzeit des Abrufs
- Meldung, ob der Abruf erfolgreich war
- Bearbeitungsdauer des Requests in Mikrosekunden
- Verwendeter Useragent
- Verwendete SSL-Version
- Referrer
- Zustelladresse
- E-Mail-Adresse
- Telefonnummer

4 Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Für die vorliegende Datenschutz-Folgenabschätzung sind in der Prüfung der rechtlichen Zulässigkeit des ID Austria Systems in erster Linie die DSGVO sowie das nationale DSG in Betracht zu ziehen.

Für die Verhältnismäßigkeits- und Erforderlichkeitsprüfung ist weiters zu beachten, dass mit steigendem Umfang der Datenverarbeitung und der damit einhergehenden Intensität des Eingriffs in die Rechte und Freiheiten der betroffenen Personen, auch die Anforderungen an die Wertigkeit, der mit der Datenverarbeitung verfolgten Zwecke steigen.[144]

Im Zuge der Bewertung der Notwendigkeit und Verhältnismäßigkeit gem Art 35 Absatz 7 lit b DSGVO sind den Empfehlungen der Artikel-29-Datenschutzgruppe zufolge ua die folgenden normativen Anforderungen zu berücksichtigen:

- festgelegte, eindeutige und legitime Zwecke (Art 5 Absatz 1 lit b)
- Rechtmäßigkeit der Verarbeitung (Art 6)
- Daten, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind (Art 5 Absatz 1 lit c)
- begrenzte Speicherfrist (Art 5 Absatz 1 lit e)

Zudem ist auf Maßnahmen im Sinne der Rechte der Betroffenen einzugehen; hierzu zählen:

- Informationspflichten gegenüber den Betroffenen (Art 12, 13 und 14)
- Auskunftsrecht und Recht auf Datenübertragbarkeit (Art 15 und 20)
- Recht auf Berichtigung und Löschung (Art 16, 17 und 19)
- Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Artikel 18, 19 und 21)
- Verhältnis zu *Auftragsverarbeitern* (Art 28)
- Garantien in Bezug auf die internationale Übermittlung von Daten[145]

[144] Vgl *Trieb* in *Knyrim*, DatKomm (2019) Art 35 Rz 112; siehe auch *Bock* et al, Datenschutz-Folgenabschätzung für die Corona-App (2020) 60 ff.

[145] Siehe *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01 (2017) 28 f.

4.1 Was sind personenbezogene Daten?

Gemäß Art 4 Z 1 DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen; (...)". Gemäß ErwGr 26 fallen darunter auch pseudonymisierte Daten.

Die Definition des Begriffs „personenbezogene Daten" ist somit sehr weit gefasst, denn er umfasst dem Wortlaut zufolge alle Informationen, die sich auf eine natürliche Person beziehen.[146] Daher gibt es ab Vorliegen der Identifizierbarkeit einer natürlichen Person keinerlei qualitative oder quantitative Einschränkungen für die Qualifikation von personenbezogenen Daten. Es kann sich dabei um persönliche Informationen wie Name und Anschrift, also herkömmliche Bestandsdaten, ebenso handeln wie um äußere Merkmale wie Geschlecht, Größe und Gewicht, oder innere Zustände iSv Überzeugungen und Meinungen.[147] Auch sachliche Informationen wie Vermögens- und Eigentumsverhältnisse und sonstige Beziehungen der Person zu *Dritten* können als personenbezogene Daten gem Art 4 Z 1 DSGVO qualifiziert werden.[148]

Vor allem auch in Bezug auf Datenverarbeitungen durch sogenannte intelligente Endgeräte, wie Smartphones und Tablets, ist zu berücksichtigen, dass Standortinformationen, eindeutige Geräte- und Kundenkennungen (wie zB IMEI[149], IMSI[150], UDID[151], MSISDN[152]), die Identität des Telefons[153], Kreditkarten- und Zahlungsdaten oder auch der Browserverlauf laut Stellungnahme 02/2013 der Artikel-29-Datenschutzgruppe als personenbezogene Daten zu werten sind.[154] Weitere gängige Angaben sowie Kennziffern bzw Chiffren mit identifizierendem Bezug zu einer natürlichen Person sind zB Name, Adresse, Handynummer[155], E-Mail-Adresse, Sozialversicherungsnummer[156], KFZ-Kennzeichen[157], IP-Adresse[158] und auch medizinische Diagnosen.[159]

Die Qualifikation von personenbezogenen Daten gem Art 4 Z 1 DSGVO hängt im Wesentlichen von vier Faktoren ab: Information, Personenbezug, natürliche Person und Identifizierung bzw Identifizierbarkeit.[160] Die Information kann sich zusammensetzen aus sachbezogenen Aussagen zu Verhältnissen oder überprüfbaren Eigenschaften sowie Einschätzungen und Urteilen über die betroffene Person. Der Personenbezug von Daten kann wiederum durch jene Information hergestellt werden, welche ein Inhaltselement, Zweckelement oder Ergebniselement beinhaltet. Der dritte wesentliche Faktor bei der Qualifikation von personenbezogenen Daten gem Art 4 Z 1 DSGVO richtet sich auf die betroffene Person, bei der es sich immer um eine natürliche Person handeln muss. Der

---

[146] *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9 DSGVO (Stand 1. 12. 2018, rdb.at).
[147] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO² Art 4 Nr 1 Rz 8.
[148] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO² Art 4 Nr 1 Rz 8.
[149] *International Mobile Equipment Identity* – eindeutige Nummer des Endgeräts.
[150] *International Mobile Subscriber Identity*– eindeutige Nummer des Netzteilnehmers.
[151] *Unique Device Identifier*– eindeutige Gerätenummer für Apple-Produkte.
[152] *Mobile Station Integrated Services Digital Network* – weltweit eindeutige Mobilfunk-Rufnummer.
[153] Nutzer von intelligenten Endgeräten können diese idR auch selbst benennen, wobei sie zumeist unter Verwendung ihres eigenen Namens benannt werden, wie zB „Maximilian Musterfrau's iPhone".
[154] *Artikel-29-Datenschutzgruppe,* Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, WP 202 (2013) 10 f.
[155] *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013, 10.
[156] Vgl DSK 12. 11. 2004, K120.902/0017-DSK/2004; BVwG 11.06.2018, W211 2161456-1.
[157] Vgl VfGH 15. 6. 2007, G 147/06; DSK 11.7.2008, K121.359/0016-DSK/2008.
[158] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[159] *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9 DSGVO.
[160] Vgl *Klabunde* in *Ehmann/Selmayr*, DS-GVO² Art 4 Rz 8.

vierte und letzte wesentliche Faktor der Begriffsbestimmung „personenbezogener Daten“ ist die Identifizierung bzw Identifizierbarkeit. Bei der vorliegenden Identitätskomponente bedarf es einer klaren Abgrenzung zwischen den sogenannten primären Identifikationsmerkmalen und jenen Daten, die für die Identifizierbarkeit einer natürlichen Person geeignet sind.

Informationen, aus denen die Identität der Person unmittelbar hervorgeht, werden primäres Identifikationsmerkmal bezeichnet.[161] Wird bspw der Name einer Person verarbeitet, handelt es sich hierbei um ein personenbezogenes Datum, da Personen im Alltag idR bereits durch die Angabe ihres Vor- und Nachnamens eindeutig identifiziert sind.[162] Dies hat zur Folge, dass sämtliche weiteren Informationen, die direkt einer identifizierten Person zuordenbar sind, als personenbezogene Daten gem Art 4 Z 1 DSGVO zu werten sind.

Die Identifizierbarkeit richtet sich gem Art 4 Z 1 2. Halbsatz DSGVO wiederum danach, ob eine natürliche Person „[…] direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“. Die Identifikation einer Person kann somit auch als ein Akt der eindeutigen Zuordnung und bestätigenden Wiedererkennung gewertet werden.

Kann somit eine natürliche Person nicht direkt, sondern nur indirekt über zusätzliches Wissen, identifiziert werden, gilt diese lediglich als identifizierbar. Dies trifft ebenso auf pseudonymisierte Daten gem Art 4 Z 5 DSGVO zu, wobei hier die notwendigen Zusatzinformationen gesondert aufbewahrt sowie technischen und organisatorischen Maßnahmen zu unterliegen haben, um zu gewährleisten, dass die betreffenden Daten eben nicht einer identifizierten oder identifizierbaren Person zugewiesen werden können.

Gem ErwGr 26 sollten „[b]ei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, [...] alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.

Die Literatur[163] und unionsrechtliche Judikatur[164] setzen am sogenannten relativen Personenbezug bzw der relativen Theorie[165] an, wonach für die Bestimmung der Identifizierbarkeit die Kenntnisse und Mittel der datenverarbeitenden Stelle und nicht irgendeines *Dritten* ausschlaggebend sind. Sofern der

[161] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[162] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO/BDSG[2] Art 4 Nr 1 Rz 18; *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 17.
[163] Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20; *Hödl* in *Knyrim,*DatKomm Art 4 Rz 14; eher für die relative Theorie, allerding teils differenzierte Ansicht *Ziebarth* in *Sydow*, Europäische Datenschutzgrundverordnung[2] Art 4 Rz 33 ff.
[164] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[165] Vgl *Hödl* in *Knyrim,* DatKomm Art 4 Rz 14; *Klar/Kühling* in *Kühling/Buchner* DS-GVO/BDSG[2] Art 4 Nr 1 Rz 26 ff; *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.

Verantwortliche Einzelangaben einer Person durch relevantes Zusatzwissen[166] [ggf auch von ihm zurechenbaren (Sub-)*Auftragsverarbeiter*] direkt zuordnen kann, ist die Identifizierbarkeit zu bejahen; dadurch sind diese Einzelangaben für die datenverarbeitende Stelle als personenbezogene Daten gem Art 4 Z 1 DSGVO zu qualifizieren.[167] Selbige Auffassung vertrat der EuGH in der Rechtssache C-582/14 zum Urteil *Breyer* gegen BRD, wonach dynamische IP-Adressen einer natürlichen Person für die Anbieter*innen als personenbezogene Daten gem Art 4 Z 1 DSGVO (ex-Art 2 lit a EG-DSRL) zu beurteilen sind, sofern *der Anbieter* „über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, (…), bestimmen zu lassen."[168]

4.1.1 Datenstrukturen und eindeutige Identifikatoren im ID Austria System

Die ID Austria (bzw der E-ID) ist gem § 2 Z 10 E-GovG eine „logische Einheit", die eine qualifizierte elektronische Signatur mit einer Personenbindung sowie den zugehörigen Sicherheitsdaten und -funktionen verbindet. Sie dient dem Nachweis der eindeutigen Identität, weiterer (Personen)Merkmale sowie des Bestehens einer Einzelvertretungsbefugnis eines *Einschreiters* und der Authentizität eines elektronisch gestellten Anbringens.[169] Bewirkt wird die eindeutige Identifikation[170] einer natürlichen Person mittels ID Austria durch die sogenannte Personenbindung, welche durch die Stammzahlenregisterbehörde (SZRB) erfolgt. Dabei wird dem *ID-Inhaber* von der SZRB elektronisch signiert oder besiegelt bestätigt, dass ihm ein oder mehrere bereichsspezifische Personenkennzeichen (bPK) zugeordnet sind. Die Personenbindung wird bei öffentlichen SP[171] und bei eIDAS[172] mit dem Minimal Dataset (MDS), bestehend aus dem Vor-, Nachname und Geburtsdatum und dem bPK, im Fall privater SP nur mit dem bPK ohne MDS,[173] verbunden, wodurch die SZRB auch die Richtigkeit der Zuordnung bestätigt. Über das MDS hinaus können mit Einwilligung der Benutzer*innen in die Personenbindung auch weitere Merkmale iSv Personenmerkmalen, Attributen bzw personenbezogenen Daten eingefügt werden.

Nach Maßgabe des E-GovG verwendet das ID Austria System zur eindeutigen Identifizierung von Personen sowie für die Übermittlung von verschlüsselten und signierten Personenmerkmalen nach einer erfolgreichen Anmeldung mit der ID Austria verschiedene Datenstrukturen, auf welche nachfolgend überblicksartig eingegangen wird:

Bei der sogenannten Online-Personenbindung[174] handelt es sich um eine eindeutige Bindung des qualifizierten Signaturzertifikats einer Person zu ihrer Stammzahl (SZ). Diese **Personenbindung** wird bei jedem Anmeldevorgang neu erstellt und von der SZRB signiert, um so die Aktualität und Richtigkeit der in der Personenbindung enthaltenen Daten zu wahren. Dabei wird die verschlüsselte Stammzahl

[166] Ob zudem unter der DSGVO noch das Kriterium „rechtlich zulässige Mittel" zu berücksichtigen ist, ist nicht völlig geklärt, krit *Karg* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 4 Nr 1 Rz 64; deutlicher *Brauneck*, EuZW 2019, 680 (688).
[167] Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.
[168] EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779, Rz 65.
[169] Gem § 4 Abs 1 E-GovG.
[170] Gem § 2 Z 4 E-GovG mit Verweis auf Art 3 Z 1 eIDAS-VO, womit die tatsächliche elektronische Identifizierung gemeint ist.
[171] Siehe § 4 Abs 5 E-GovG.
[172] Siehe § 14a Abs 2 E-GovG.
[173] Siehe § 14 Abs 3 E-GovG.
[174] *A-SIT/EGIZ*, ID Austria – Technisches Whitepaper – Hintergrundinformationen 23.

(vSZ) der Person mit ihrem qualifizierten Signaturzertifikat und weiteren Identitätsmerkmalen verknüpft.

Anzumerken ist dabei, dass man unter einer **Verschlüsselung** jenen Vorgang versteht, bei dem Informationen mit Hilfe eines kryptographischen Verfahrens bzw eines Schlüssels in eine unleserliche Geheimschrift umgewandelt werden, welche nur unter Verwendung des jeweiligen Entschlüsselungsschlüssels wieder lesbar wird.[175] Der Personenbezug von Daten wird allerdings durch das jeweilige Verschlüsselungsverfahren nicht geschmälert, da die datenverarbeitende Stelle auch weiterhin den Personenbezug herstellen kann.[176] Somit handelt es sich bei der Verschlüsselung von personenbezogenen Daten lediglich um eine technische Sicherheitsmaßnahme iSd technischen und organisatorischen Maßnahmen (TOMs) gem Art 32 DSGVO, die nach Maßgabe der relativen Theorie zwar der Identifizierbarkeit der betroffenen Person für die datenverarbeitende Stelle nicht entgegensteht, jedoch die unberechtigte Kenntnisnahme *Dritter* deutlich erschwert,[177] und daher zum Schutz personenbezogener Daten wesentlich beiträgt.

Letztendlich basiert die eindeutige Identifizierung von Bürger*innen im ID Austria System auf **Zertifikatsbindungen**, die den Identifikator der Benutzer*innen (also der vSZ) mit dem öffentlichen Schlüssel eines Signaturzertifikats verknüpfen. Konkret wird zwischen drei verschiedenen ID Austria Zertifikatsbindungen unterschieden, nämlich dem sogenannten qcBind[178], bcBind[179] und eIDASBind[180], wobei jede dieser Zertifikatsbindungen den eindeutigen Identifikator (vSZ) mit einem anderen öffentlichen Signaturschlüssel verknüpft. In allen drei möglichen Ausprägungen inkludiert die jeweilige Zertifikatsbindung (a) den öffentlichen Schlüssel (Public Key) eines Signaturzertifikats, (b) die verschlüsselte Stammzahl (vSZ), (c) den aktuellen Status der ID Austria (Basis ID Austria / ID Austria) und (d) den Ländercode des Quelllands der elektronischen Identität der Person. Sämtliche Zertifikatsbindungen werden von der SZRB zum Schutz der Authentizität und Integrität all jener Daten, die in der Personenbindung enthaltenen sind, signiert.

Immanenter Bestandteil der ID Austria sind die **Stammzahl (SZ)** und das **bereichsspezifische Personenkennzeichen (bPK)** als eindeutige Identifikatoren, auf welche nachfolgend näher eingegangen wird:

Die Basis zur Erstellung der ID Austria ist die in Bezug auf eine Person eindeutig zugewiesene **ZMR-Zahl** (auch Basiszahl genannt), die neben personenbezogenen Daten wie Vor-, Nachname und Geburtsdatum der jeweiligen Person im ZMR registriert ist. Sofern eine Person keinen Wohnsitz in Österreich hat, verfügt sie dahingehend auch über keinen ZMR-Eintrag und keine ZMR-Zahl. Jedoch

[175] *Jandt* in *Kühlinger/Buchner*, DS-GVO 607 Rz 19.
[176] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.
[177] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.
[178] Diese Zertifikatsbindung wird bei der Registrierung/Aktivierung der ID Austria erstellt – näheres hierzu, siehe *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 23.
[179] Diese Zertifikatsbindung wird bei der Erstellung einer kryptographischen Bindung zum IDP, die für eine spätere vereinfachte Weiterverwendung der ID Austria verwendet werden kann, generiert – näheres hierzu, siehe *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 23 f.
[180] Diese Zertifikatsbindung wird im Zuge einer Authentifizierung über das eIDAS-Framework am zentralen österreichischen eIDAS-Knoten generiert – näheres hierzu, siehe *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 24.

kann sich eine solche natürliche Person, die dennoch elektronische Services des österreichischen E-Government nutzen möchte, im Ergänzungsregister für natürliche Personen (ERnP) eingetragen lassen.[181] Dieser Person wird dann im ERnP eine sogenannte Ordnungsnummer zugewiesen, die im Rahmen des ID Austria System dieselbe Funktion wie die ZMR-Zahl hat.

Da die Verwendung eines einzigen Identifikators einen Rückschluss auf die Nutzung aller elektronischen Services durch eine Person leicht ermöglichen würde, darf die ZMR-Zahl (oder Ordnungsnummer) auch nicht zur Identifizierung von Benutzer*innen bzw Bürger*innen in behördlichen elektronischen Prozessen verwendet werden. Um in diesem sensiblen Bereich des Identitätsmanagements bereits innerhalb des ID Austria Systems Tracking zu verhindern, wird daher die ZMR-Zahl lediglich zur Berechnung der sogenannten Stammzahl (SZ) herangezogen. Diese wird wiederum in weiterer Folge zur Berechnung des bereichsspezifischen Personenkennzeichens (bPK) verwendet, mit dem der jeweilige öffentliche oder private Service Provider von dem ID Austria System als eindeutiger Identifikator des *ID-Inhabers* versorgt wird.

Die **SZ** ist der eindeutige und persistente Identifikator von Benutzer*innen und wird direkt von ihrer ZMR-Zahl (oder Ordnungsnummer) abgeleitet. Für die Berechnung der SZ wird ein symmetrischer Verschlüsselungsalgorithmus verwendet. Die Berechnung wird ausschließlich von der SZRB unter Verwendung eines geheimen und nur der SZRB bekannten kryptographischen Schlüssels durchgeführt. Mit Hilfe dieses Schlüssels verschlüsselt die SZRB die ZMR-Zahl (oder Ordnungsnummer) der Benutzer*innen; das Resultat dieser Verschlüsselungsoperation ist die SZ. Da nur die SZRB den verwendeten Schlüssel kennt, ist auch nur diese in der Lage, aus der SZ wieder auf die ZMR-Zahl (oder Ordnungsnummer) zurückzurechnen. Die Berechnung der SZ findet über das Stammzahlenregister (SZR) statt, welches im Auftrag der SZRB (bzw des BMDW) vom BMI als *Auftragsverarbeiter,* welcher auftragsgemäß die Berechnung der SZ durchzuführen hat, betrieben wird.

Gem § 6 Abs 1 E-GovG erfolgt die eindeutige Identifikation von Betroffenen bzw Benutzer*innen lediglich „auf Basis ihrer Stammzahl“, da nämlich die SZ natürlicher Personen nach § 12 E-GovG einem besonderen Schutz unterliegt und außerhalb des Errechnungsvorgangs nicht gespeichert werden darf. Eine direkte Verwendung der SZ von natürlichen Personen zu deren Identifizierung bei Service Providern ist folglich rechtlich nicht zulässig, da dies ein Tracking von Personen über Service Provider-Grenzen hinweg ermöglichen würde. Deshalb werden öffentliche sowie private Service Provider von dem ID Austria System nicht mit der SZ des *ID-Inhabers*, sondern mit dem **bereichsspezifischen Personenkennzeichen (bPK)**, für deren Berechnung die SZ als Teil des Basiswerts dient, als eindeutige Identifikatoren versorgt. Zur Erreichung einer eindeutigen Identifikation einer natürlichen Person im ID Austria System wird somit nicht die SZ selbst, sondern eine Ableitung auf Basis der Stammzahl mittels bPK herangezogen.[182] Dabei ist davon auszugehen, dass bereichsspezifische Personenkennzeichen indirekte personenbezogene Daten bzw pseudonymisierte Daten iSd Art 4 Z 5 DSGVO darstellen, sofern sie nicht ohnehin mit Identitätsdaten von Betroffenen verbunden sind.[183]

[181] Allenfalls auch im Zuge der Registrierung des E-ID bzw der ID Austria oder es erfolgt eine automatische Eintragung im Ergänzungsregister für natürliche Personen (ERnP) durch die Verwendung einer eIDAS-konformen ausländischen eID bei einem österreichischen Service Provider.
[182] Vgl *Spornberger* in *Zankl*, Rechtshandbuch der Digitalisierung (2021) Rz 17.50.
[183] Vgl DSB 10. 7. 2014, DSB-D121.921/0001-DSB/2014.

Ein Bereich bezeichnet bei Service Providern des öffentlichen Sektors einen Bereich der öffentlichen Verwaltung (zB Gesundheit, Finanzen, etc). Die verschiedenen öffentlichen Bereiche sind in der E-Government-Bereichsabgrenzungsverordnung (E-Gov-Ber-AbrV) definiert. Daraus gehen die sogenannten Bereichskürzel für den jeweiligen Bereich des öffentlichen Service Providers hervor. Bei privatwirtschaftlichen Service Providern ergibt sich für jede Organisation (Unternehmen, Verein, etc - iSv Service Owner) ein eigener Bereich. Das Bereichskürzel des Service Owner ist dessen Stammzahl bzw je nach Rechtsform dessen FB-Nummer, ZVR-Nummer oder Ordnungsnummer. Es wird somit jeder Bereich mit einem anderen bPK für dieselbe Person versorgt, womit die Verhinderung von Tracking über Bereichsgrenzen hinweg gewährleistet werden soll.

So wie in den Gesetzesmaterialien[184] zum E-GovG hierzu erläutert wurde, werden alle bPK über eine Einwegfunktion (iSe kryptographischen Einwegableitung) von der SZ der Bürger*innen bzw Benutzer*innen abgeleitet und stellen einen eindeutigen und persistenten Identifikator dar, der vom Service Provider zur Identifizierung der Benutzer*innen verwendet werden kann. In die Ableitung des bPK von Benutzer*innen geht neben deren SZ auch ein Identifikator jenes Bereichs ein, für den das bPK berechnet wird. Die zum Einsatz kommende kryptographische Einwegableitung soll daher die Erreichung der vorgesehenen Effekte bewirken, nämlich (a) die Unumkehrbarkeit der Ableitung, dh aus einer Ableitung der SZ iSd bPK darf die SZ nicht errechnet werden können, und (b) vom bPK eines Bereichs darf nicht auf die bPK eines anderen Bereichs geschlossen werden können. Zuständig für die Berechnung von bPK ist grds ebenfalls die SZRB, da nur diese über die unverschlüsselte SZ der Benutzer*innen verfügt. Jedoch bedient sich die SZRB gem § 7 Abs 2 E-GovG auch bei der Berechnung der bPK für die Erstellung der Personenbindung des BMI als *Auftragsverarbeiter*.

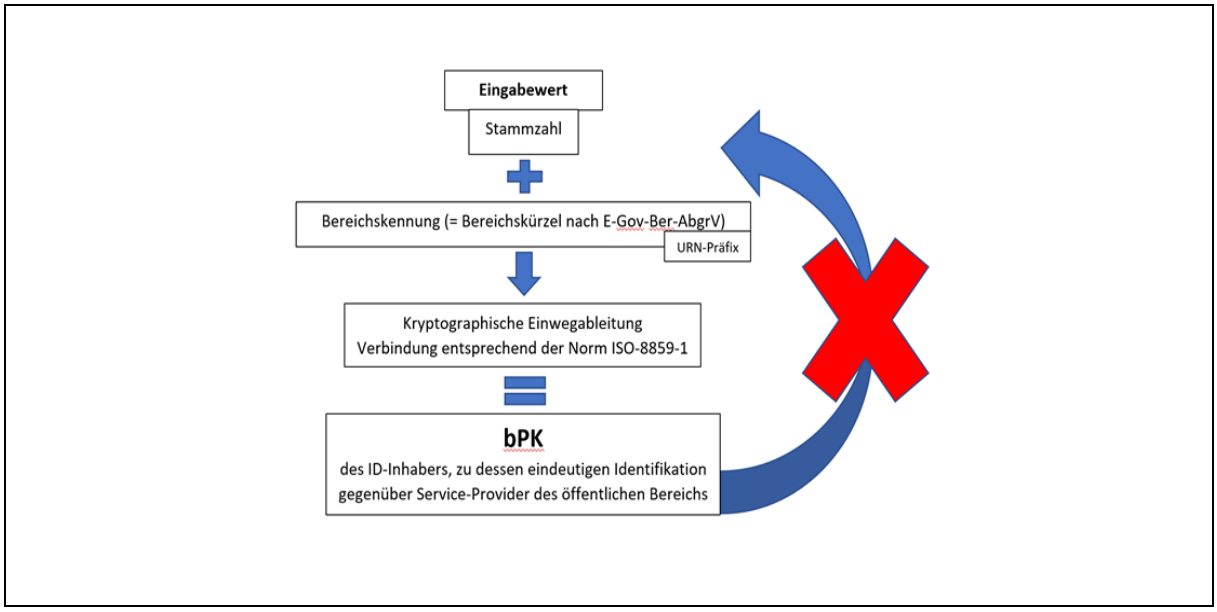

Abbildung 3: Hash-Funktion – Berechnung bPK für öffentlichen Bereich[185]

[184] ErläutRV 252 BlgNR 22. GP 8.
[185] Näheres hierzu, siehe *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 18.

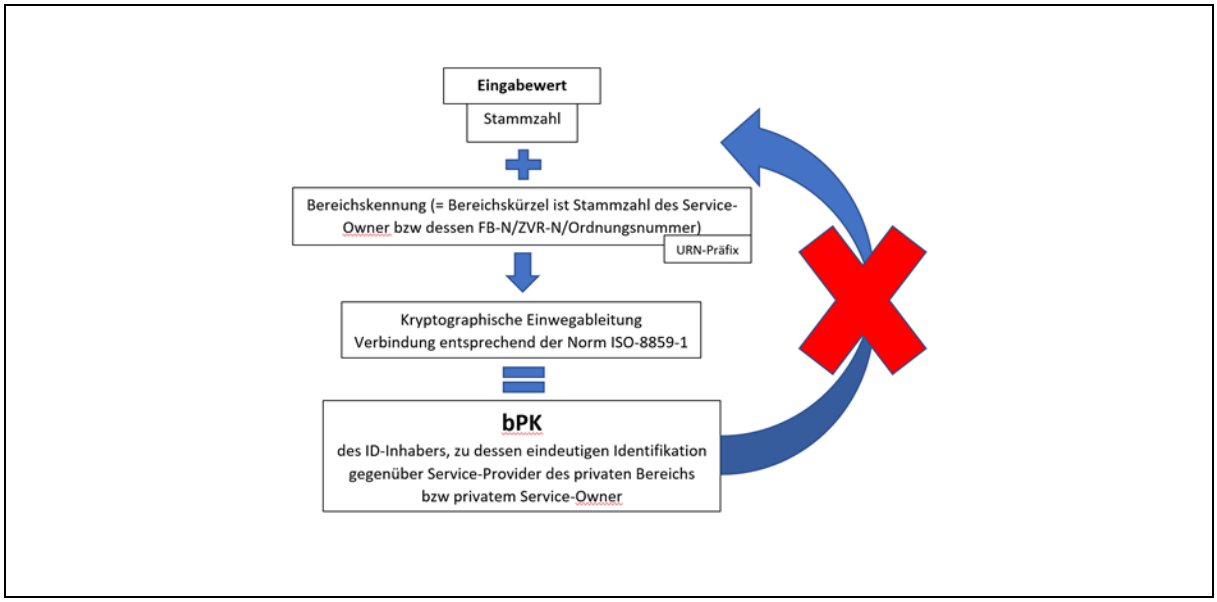

Abbildung 4: Hash-Funktion – Berechnung bPK für privaten Bereich[186]

Zusammenfassend kann daher festgehalten werden, dass die ID Austria iSe E-ID bzw elektronischen Identitätsnachweises gem § 2 Z 10 E-GovG als personenbezogenes Datum gem Art 4 Z 1 DSGVO zu qualifizieren ist, da die eindeutige elektronische Identifikation der Benutzer*innen gegenüber den jeweils durch das ID Austria System berechtigten datenverarbeitenden Stellen bewirkt werden soll.[187]

Hinsichtlich der zwei wesentlichen Identifikatoren, nämlich der SZ und dem bPK ist festzuhalten, dass auch diese als personenbezogene Daten gem Art 4 Z 1 DSGVO zu qualifizieren sind. Sie werden jedoch beide durch die Anwendung von Verschlüsselungsverfahren erzeugt, um so zum Schutz personenbezogener Daten innerhalb der betreffenden Verarbeitungstätigkeiten im ID Austria System beizutragen. Insgesamt zeigt sich, dass die Architektur des ID Austria Systems über die implementierten Vorgänge und Verschlüsselungsverfahren auf ein hohes Maß an Pseudonymisierung abzielt.

[186] Näheres hierzu, siehe *A-SIT/EGIZ*, ID Austria - Technisches Whitepaper - Hintergrundinformationen 18.
[187] Vgl hierzu auch *Commonwealth Digital Transformation Agency (DTA)*, Initial Privacy Impact Assessment (2016) 32; https://www.dta.gov.au/sites/default/files/files/digital-identity/PIAs/DTA_TDIF_Alpha_Initial_PIA.pdf (abgerufen am 22.04.2022).

4.2 Rechtsgrundlagen

4.2.1 Regelungssystematik der DSGVO

Die aus der DSGVO abzuleitende Regelungssystematik in Bezug auf die Rechtsgrundlagen sieht vor, dass jegliche Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, ein Erlaubnistatbestand bzw eine Rechtsgrundlage der Art 6, 9 bzw 10 DSGVO rechtfertigen die betreffende Datenverarbeitung.[188] Für die Verarbeitung von personenbezogenen Daten gem Art 4 Z 1 DSGVO enthält Art 6 Abs 1 DSGVO eine taxative Liste von sechs Erlaubnistatbeständen:

- Die Einwilligung der betroffenen Person für einen oder mehrere bestimmte Zwecke (lit a)
- Das Vorliegen eines Vertrags, oder die Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person (lit b)
- Die Erfüllung einer gesetzlichen Verpflichtung des *Verantwortlichen* (lit c)
- Die Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines *Dritten* (lit d)
- Die Erforderlichkeit für eine Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem *Verantwortlichen* übertragen wurde (lit e)
- Die Erforderlichkeit zur Wahrung der berechtigten Interessen des *Verantwortlichen* oder eines *Dritten* (lit f)

Art 9 Abs 2 DSGVO enthält die taxative Liste jener zehn Erlaubnistatbestände, auf welche die Verarbeitung besonderer Kategorien personenbezogener Daten (kurz: sensibler Daten) gestützt werden kann:[189]

- Die ausdrückliche Einwilligung der betroffenen Person (lit a)
- Die Erforderlichkeit zur Erfüllung von Pflichten oder Ausübung von Rechten im Arbeits- und Sozialrecht (lit b)
- Die Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten, ohne erteilter Einwilligung (lit c)
- Interne Verarbeitung durch Organisationen ohne Gewinnerzielungsabsicht (lit d)
- Die Verarbeitung von offensichtlich durch die betroffene Person selbst öffentlich gemachten Daten (lit e)
- Die Erforderlichkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte (lit f)
- Die Erforderlichkeit aus Gründen eines erheblichen öffentlichen Interesses (lit g)
- Die Erforderlichkeit für Zwecke des Gesundheits- oder Sozialwesens (lit h)
- Die Erforderlichkeit aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (lit i)
- Die Erforderlichkeit für im öffentlichen Interesse liegende Archiv-, Forschungs- oder statistische Zwecke (lit j)

[188] Vgl *Feiler/Forgó*, EU-DSGVO Art 6 Anm 1.
[189] Gem Art 9 Abs 1, Art 4 Z 13 - 15 DSGVO.

4.2.2 Datenverarbeitung zum Zwecke der Registrierung und Akkreditierung privater Service Provider

Die Verarbeitung personenbezogener Daten stützt sich in diesem Fall auf Art 6 lit e DSGVO. Diese Bestimmung legt fest, dass die Verarbeitung rechtmäßig ist, wenn sie zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem *Verantwortlichen* übertragen wurde, erfolgt, erforderlich ist.

Eine solche Rechtsgrundlage muss dabei durch Unionsrecht oder das Recht des betreffenden Mitgliedstaats, dem der *Verantwortliche* unterliegt, festgelegt werden. Art 6 Abs 1 lit e steht in einem engen Zusammenhang mit Art 6 Abs 2 und 3, wonach der Zweck zur Erfüllung der gesetzlich übertragenen Aufgabe notwendig sein muss. Letztere muss in der Rechtsgrundlage hinreichend bestimmt beschrieben werden. Da Art 6 Abs 1 lit e ein sehr weit gefächertes Anwendungsspektrum besitzt, ist laut Artikel-29-Datenschutzgruppe „eine strenge Auslegung und eine klare Benennung des gegebenen öffentlichen Interesses und der öffentlichen Gewalt, die die Verarbeitung rechtfertigen, auf Einzelfallbasis geboten."[190]

§ 18 Abs 2 E-GovG iVm § 18 Abs 5 E-GovG regelt die Einbindung der Service Provider. Für die Nutzung des E-ID Systems haben sich private Service Provider beim Bundesminister für Inneres zu registrieren, welcher in weiterer Folge auch über die Eröffnung oder Unterbindung der Nutzung des E-ID Systems entscheidet.

Zur Zweckbestimmung und Notwendigkeit der Norm wird in den Gesetzesmaterialien[191] wie folgt ausgeführt:

„Voraussetzung für eine Teilnahme am E-ID-System ist wie bisher die Überprüfung, ob der Dritte im Sinne des Z 3 personenbezogene Daten bisher auf rechtmäßige Weise und nach Treu und Glauben verarbeitet hat. Um dies zu gewährleisten, soll in Abs. 2 eine Mitwirkungspflicht des Dritten im Sinne des Abs. 1 Z 3 derart normiert werden, dass dieser dem Bundesminister für Inneres jeden Umstand bekanntzugeben hat, der einer Nutzung des E-ID-Systems entgegensteht. Zur Überprüfung, ob der Dritte im Sinne des Abs. 1 Z 3 personenbezogene Daten bisher nach Treu und Glauben und auf rechtmäßige Weise verarbeitet hat, soll der Bundesminister für Inneres gemäß Abs. 2 Z 1 in Bezug auf die Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 (VStG), BGBl. Nr. 52/1991, eine Abfrage des Strafregisters über nicht getilgte strafgerichtliche Verurteilungen durchführen dürfen. Eine Verurteilung des Verantwortlichen gemäß § 9 VStG wegen widerrechtlichen Zugriffes auf ein Computersystem (§ 118a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974), Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) oder wegen des missbräuchlichen Abfangens von Daten (§ 119a StGB) lässt jedenfalls den Schluss zu, dass dieser Verantwortliche gemäß § 9 VStG personenbezogene Daten bisher nicht nach Treu und Glauben und auf rechtmäßige Weise verarbeitet hat.

Eine weitere wesentliche Voraussetzung für die Eröffnung der Nutzung durch den Bundesminister für Inneres ist die Glaubhaftmachung eines eigenen Zwecks. Ein solcher Zweck kann beispielsweise in einem Vorhaben eines Verkehrsverbunds bestehen, seinen Fahrgästen mit Hauptwohnsitz in einer

[190] Vgl *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO Rz 45 ff (Stand 7. 5. 2020, rdb.at).
[191] ErläutRV 469 BlgNR 27. GP 7 f.

bestimmten Gemeinde ein ermäßigtes Jahresticket anzubieten. Vom glaubhaft gemachten Zweck hängen naturgemäß auch die Datenarten ab, die vom Betroffenen angefordert werden. Es ist zu beachten, dass der Zweck der bloßen Weitergabe von empfangenen Datensätzen für eine solche Glaubhaftmachung nicht ausreicht.

Sofern durch Dritte im Sinne des Abs. 1 Z 3 im Zuge der Antragstellung eine Gewerbeinformationssystem Austria-Zahl (GISA-Zahl) angegeben wurde, soll der Bundesminister für Inneres gemäß Abs. 2 Z 2 den Inhalt der jeweiligen Gewerbeberechtigung aus dem Gewerbeinformationssystem Austria (GISA) abfragen können. In weiterer Folge wird diese Information zur Überprüfung herangezogen, ob der glaubhaft gemachte Zweck zur Nutzung des E-ID mit dem Inhalt der Gewerbeberechtigung vereinbar ist.

[...]

Gemäß Z 2 [des § 18 Abs 5, Anmerkung] ist zur Durchführung einer Abfrage des Strafregisters gemäß Abs. 2 Z 1 die Nennung der Verantwortlichen gemäß § 9 VStG, die zur Vertretung nach außen befugt sind, erforderlich. Die Angabe des Unternehmensgegenstands oder Vereinszwecks (Z 5) [des § 18 Abs 5, Anmerkung] dient der Überprüfung der Nachvollziehbarkeit der ausgewählten Merkmale, die der Betroffene Dritten im Sinne des Abs. 1 Z 3 nachweisen kann, da daraus maßgebliche Rückschlüsse auf die für diesen Bereich relevanten personenbezogenen Daten gezogen werden können. Sofern vorhanden, soll auch die GISA-Zahl gemäß Z 4 anzugeben sein, damit der Bundesminister für Inneres in weiterer Folge den Inhalt der Gewerbeberechtigung aus dem GISA abfragen kann (Abs. 2 Z 2). Zudem soll im Zuge der Zustimmung zur Weitergabe an Dritte nach Abs. 1 Z 3 dem E-ID-Inhaber das gemäß Z 4 anzugebende Logo angezeigt werden, um eine größtmögliche Transparenz in Bezug auf den Übermittlungsempfänger (den Unternehmer oder den Verein) sicherzustellen. Die verpflichtende Angabe einer Telefonnummer und E-Mail-Adresse soll die Kontaktaufnahme zum Unternehmen oder Verein erleichtern und eine möglichst rasche Bearbeitung von Anbringen gewährleisten. Zudem sollen Dritte im Sinne des Abs. 1 Z 3 über wichtige Informationen betreffend die Nutzung des E-ID-Systems, etwa die Verfügbarkeit zusätzlicher weiterer Merkmale im Sinne der § 4 Abs. 2 und § 14 Abs. 3 oder die Durchführung von Wartungsarbeiten, zeitnah und unkompliziert verständigt werden. Schließlich haben Unternehmer und Vereine im Zuge der Antragstellung die für die Nutzung des E-ID-Systems glaubhaft gemachten Zwecke anzugeben.“[192]

4.2.3 Datenverarbeitung zum Zweck der Registrierung der Benutzer*innen

Die Verarbeitung personenbezogener Daten stützt sich auch in diesem Fall auf Art 6 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Hinsichtlich der Verarbeitung des Lichtbildes ist § 4b Abs 1 Z 8 E-GovG bzw. § 4a Abs 4 E-GovG, hinsichtlich sonstiger personenbezogener Daten § 4a E-GovG iVm § 4b Abs 1 und 3 E-GovG die nationale Rechtsgrundlage.

[192] Als Rechtsgrundlage zur Registrierung behördlicher Service Provider dient § 10 Abs 1 S 2 E-GovG. Für weitere Informationen zum Registrierungsprozess von öffentlichen bzw. behördlichen Service-Providern siehe https://eid.egiz.gv.at/anbindung/registrierung/registrierung-von-behoerdlichen-service-providern/ (abgerufen am 22. 04. 2022).

Zur Zweckbestimmung und Notwendigkeit der Norm wird in den Gesetzesmaterialien[193] wie folgt ausgeführt:

„Im Zuge der Registrierung des E-ID ist die jeweilige Registrierungsbehörde als Auftraggeber im Sinne des Datenschutzgesetzes 2000 (DSG 2000), BGBl. I Nr. 165/1999, ermächtigt, bestimmte Daten im vom Bundesministerium für Inneres betriebenen Identitätsdokumentenregister zu erfassen und zu verarbeiten (§ 4b).

Im Hinblick auf eine möglichst effiziente und rasche Abwicklung des behördlichen Registrierungsprozesses können Inhaber eines Reisepasses oder eines Personalausweises nach § 4a Abs. 3 bereits im Vorfeld die für die Registrierung erforderlichen Daten an die Behörde übermitteln (Vorregistrierung).

Die Behörde hat diese Daten aus datenschutzrechtlichen Gründen innerhalb von 30 Tagen zu löschen, sofern in diesem Zeitraum keine Registrierung des E-ID vorgenommen wurde. Entscheidende Voraussetzung für die Registrierung des E-ID ist nach § 4a Abs. 4 die Feststellung der eindeutigen Identität des Betroffenen. In diesem Zusammenhang soll im Registrierungsprozess die Möglichkeit geschaffen werden, die vorgelegten Ausweisdaten wie z. B. Reisepassnummer in den entsprechenden Registern abzufragen. Damit kann die Sicherheit bei der Identitätsfeststellung zur Registrierung des E-ID erhöht werden. Es werden dadurch auch die notwendigen Vorkehrungen getroffen, um das Risiko mindern zu können, dass die Identität der Personen nicht mit der beanspruchten Identität übereinstimmt, z. B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Beweismittel, wie es in Anhang unter Punkt 2.1.2 der Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, ABl. Nr. L 235 vom 9.9.2015 ab dem Sicherheitsniveau ‚substanziell' im Sinne der eIDAS-VO vorgesehen ist."

Die Materialien führen weiters aus:[194]

„Mit der vorgeschlagenen Regelung soll präzisiert werden, dass Inhaber eines inländischen Reisedokuments im Rahmen der Vorregistrierung eines E-ID bestimmte personenbezogene Daten den Behörden im Wege des VDA, der im Auftrag des Bundesministers für Inneres tätig wird, zur Verfügung stellen können. In diesem Zusammenhang ist besonders hervorzuheben, dass die Vorregistrierung nicht zwingend erforderlich ist, sondern freiwillig durch den Betroffenen in Anspruch genommen werden kann. Die Vor- und Familiennamen, das Geburtsdatum, die Pass- oder Personalausweisnummer sowie gegebenenfalls die bekanntgegebene E-Mail-Adresse können für eine anschließende raschere Abwicklung des Registrierungsprozesses herangezogen werden, sofern der Betroffene die Registrierung eines E-ID innerhalb von 30 Tagen ab Bekanntgabe dieser Daten durchführen lässt.

[193] ErlIA 2227 BlgNR 25. GP 7.
[194] ErläutRV 469 BlgNR 27. GP 3.

[...]

Um eine sinnvolle und praxisnahe Nutzung des E-ID zu gewährleisten, soll in Abs. 4 normiert werden, dass der E-ID-Werber grundsätzlich zur Beibringung eines Lichtbilds verpflichtet ist. Diese Verpflichtung soll jene E-ID-Werber treffen, die nicht schon ohnehin aufgrund der beabsichtigten Ausstellung eines Reisedokuments ein Lichtbild beizubringen haben oder das im Rahmen der bereits erfolgten Ausstellung eines Reisedokuments beigebrachte Lichtbild zum Zeitpunkt der Registrierung des E-ID noch die Kriterien des § 4 der Passgesetz-Durchführungsverordnung (PassG-DV), BGBl. II Nr. 223/2006, erfüllt. Insbesondere darf das entsprechende Lichtbild daher nicht älter als sechs Monate sein.

Im Hinblick auf die Möglichkeit, dass auch Fremde die Registrierung eines E-ID gemäß § 4a Abs. 2 verlangen können, ist es sachgerecht, zur Überprüfung der Identität und der vorgelegten Dokumente auch die vorhandenen Datenbestände des Zentralen Fremdenregisters gemäß §§ 26 und 27 des BFA-Verfahrensgesetzes (BFA-VG), BGBl. I Nr. 87/2012, heranziehen zu können.

Die in § 4a Abs. 4 dritter Satz vorgesehene Möglichkeit der Abfrage von Informationen aus den genannten Datenverarbeitungen dient lediglich der Überprüfung der Identität und der vorgelegten Dokumente durch die Registrierungsbehörde. Für bestimmte personenbezogene Daten, die der Behörde auf diese Weise im Zuge des Registrierungsprozesses bloß angezeigt werden, besteht in weiterer Folge die Möglichkeit, diese gemäß § 4b in der zentralen Evidenz gemäß § 22b des Passgesetzes 1992 zu verarbeiten. Hierbei handelt es sich um die Namen, das Geburtsdatum, den Geburtsort, das Geschlecht, die Staatsangehörigkeit oder die Zustelladresse (§ 4b Abs. 1 Z 1 bis 5 und Z 7). Als Zustelladresse kann beispielsweise der Hauptwohnsitz, der aus dem Zentralen Melderegister gemäß § 16 des Meldegesetzes 1991 (MeldeG), BGBl. Nr. 9/1992, abgefragt wurde, verwendet werden.

Die Möglichkeit der Übernahme dieser Daten in das IDR ist unbedingt erforderlich, um den Zeitaufwand des behördlichen Registrierungsprozesses möglichst gering zu halten. Zudem dient die Abfrage der Steigerung der Datenqualität, da etwaige Übertragungsfehler durch den Sachbearbeiter ausgeschlossen oder allenfalls auch nicht übereinstimmende Datensätze in diesen Registern bereinigt werden können. Die Richtigkeit der genannten Daten liegt auch im Interesse des E-ID-Werbers, da diese künftig mithilfe des E-ID einem Dritten gemäß § 18 Abs. 1 nachgewiesen werden können."

4.2.4 Datenverarbeitung zum Zweck der Verwendung der ID Austria

Anmeldung an Service Provider und Signatur (Verwendung):

Diese Verarbeitung personenbezogener Daten stützt sich auf Art 6 Abs 1 lit e DSGVO. Die nationalen Rechtsgrundlagen sind die §§ 4 iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[195] aus:

[195] ErläutRV 469 BlgNR 27. GP 2.

„Es soll eine Definition für den Verwendungsvorgang des E-ID eingeführt werden. Diese soll klarstellen, dass bei der Verwendung des E-ID die Erstellung einer Personenbindung entweder so wie schon derzeit mittels qualifizierter elektronischer Signatur des E-ID-Inhabers oder alternativ mittels eines sicherheitstechnisch gleichwertigen Vorgangs ausgelöst werden kann. Ein derartiger sicherheitstechnisch gleichwertiger Vorgang ist notwendig, um künftig die Smartphone-basierte Auslösung der E-ID Funktion am selben Gerät wie die Anwendung, zu der die Authentifizierung erfolgen soll, in einer sicheren Art und Weise durchführen zu können.

Die qualifizierte Signatur wird bei der Smartphone-basierten Umsetzung des Bürgerkartenkonzepts (so genannte Handy-Signatur) aktuell durch drei Faktoren ausgelöst, das Wissen des Benutzers (Passwort – Faktor 1), der Besitz des Geräts (hardwarebasiertes Element für Schlüsselaufbewahrung – Faktor 2) und eine biometrische Eigenschaft des Benutzers (aktuell Fingerabdruck und bestimmte Gesicht-Scans – Faktor 3). Der sicherheitstechnisch gleichwertige Vorgang zum Auslösen der Erstellung einer Personenbindung bei Verwendung des E-ID wird erstmalig durch eine qualifizierte Signatur des E-ID-Inhabers initiiert. Dabei wird als Sicherheitselement ein Schlüssel im hardwarebasierten Element des Geräts erstellt und der Zugriff mit einer biometrischen Eigenschaft abgesichert (äquivalent zum zweiten und dritten Faktor der qualifizierten Signatur) und durch den E-ID-Inhaber qualifiziert signiert. Dadurch entsteht eine kryptographische Bindung zwischen der qualifizierten Signatur des E-ID-Inhabers und dem erstellten Schlüssel. Die Kombination aus der kryptographischen Bindung durch die initial erstellte qualifizierte Signatur und der Verwendung des zuvor erwähnten Sicherheitselements entspricht einem sicherheitstechnisch gleichwertigen Vorgang. Das zugehörige qualifizierte Zertifikat, das für die frühere qualifizierte elektronische Signatur verwendet wurde, muss zum Zeitpunkt der jeweiligen Verwendung gültig sein.

Die biometrischen Daten werden ausschließlich gemäß den geltenden technischen Standards der Hersteller auf dem Gerät des Benutzers verarbeitet. Eine Verarbeitung dieser Daten durch die Stammzahlenregisterbehörde im Rahmen des E-ID Systems erfolgt zu keinem Zeitpunkt.

Durch diesen alternativen Vorgang kann insbesondere die mobile Verwendung des E-ID aus Nutzersicht stark vereinfacht werden, ohne sicherheitstechnische Nachteile hinnehmen zu müssen.

Ob diese alternative Verwendung für ein konkretes Verfahren ausreichend ist, hängt vom jeweiligen Verfahren, demgegenüber sich der E-ID-Inhaber authentifiziert, ab. Ist beispielsweise neben der Authentifizierung zusätzlich die eigenhändige Unterschrift für das konkrete Verfahren aufgrund anderer rechtlicher Regelungen erforderlich, so muss der E-ID jedenfalls mit einer qualifizierten elektronischen Signatur ausgelöst werden.“

Zudem führen die Materialien[196] aus:

„Bei der Verwendung der Funktion E-ID im privaten Bereich kann schon bisher ein bPK gebildet werden, wobei für die Errechnung des bPK anstelle der Bereichskennung die Stammzahl des Verantwortlichen des privaten Bereichs herangezogen wird. Dies ist somit für juristischen Personen, Vereine oder im Ergänzungsregister eingetragene Betroffene, die eine Stammzahl für den Errechnungsvorgang zur Verfügung stellen können, möglich. Um auch natürlichen Personen, die Möglichkeit zu eröffnen als Serviceanbieter unter Einsatz einer E-ID tauglichen technischen Umgebung

[196] ErläutRV 469 BlgNR 27. GP 7.

zu fungieren, soll anstelle der Stammzahl auch das bPK des Verantwortlichen des privaten Bereichs für die bPK-Errechnung herangezogen werden dürfen."

Bereitstellung von über den Minimaldatensatz hinausgehenden Attributen:

Die Datenverarbeitung stützt sich auf Art 6 Abs 1 lit a und – sofern Attribute sensible Daten beinhalten – auf Art 9 Abs 2 lit a DSGVO. Einschlägig ist § 4 Abs 2 E-GovG. Soweit im Zuge einer Anmeldung über den Minimaldatensatz hinausgehende Attribute ausgeliefert werden, ist nach Maßgabe des § 4 Abs 2 E-GovG die datenschutzrechtliche Einwilligung der Betroffenen einzuholen.

Hierzu führen die Materialien[197] aus:

„Die Einfügung weiterer Merkmale in die Personenbindung ist auch weiterhin nur mit Einwilligung des E-ID-Inhabers zulässig. Wie auch schon bisher handelt es sich dabei um eine Einwilligung gemäß Art. 4 Z 11 DSGVO. Zugänglich ist ein solches Register für die Stammzahlenregisterbehörde nur, wenn eine geeignete technische Anbindung vorhanden ist und eine entsprechende gesonderte Rechtmäßigkeit der Verarbeitung gemäß Art. 6 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) – z. B. Einwilligung – für die Weitergabe der Merkmale aus diesem Register im Wege des E-ID besteht. So könnten beispielsweise Versicherungsnachweise oder Bestätigungen über Mitgliedschaften unter Nutzung der Funktion E-ID unter Kontrolle des E-ID-Inhabers berechtigten Serviceanbietern übermittelt werden. Wie bereits im allgemeinen Teil ausgeführt, soll die Möglichkeit der Nachweise von Merkmalen aus Registern von Verantwortlichen des privaten Bereichs erst in einem nächsten Schritt technisch umgesetzt werden."

An die Freiwilligkeit von Erklärungen gegenüber hoheitlichen Stellen werden strenge Anforderungen gestellt. Soweit Betroffene bei objektiver Beurteilung damit rechnen müssen, dass ihre Zustimmung einer Form sozialen Drucks ausgesetzt und erzwungen sein könnte (öffentlich rechtliches Subordinationsverhältnis), ist die Einwilligung als Rechtsgrundlage nur eingeschränkt tauglich.[198] Das liegt nicht vor, da nur mit expliziter Einwilligung der Betroffenen Attribute übermittelt werden. Ein Erzwingen dieser Einwilligung ist weder technisch noch rechtlich vorgesehen. Zusätzlich bestätigen die Benutzer*innen jeden Login-Vorgang noch mit ihrer qualifizierten elektronischen Signatur bzw einem sicherheitstechnisch gleichwertigen Vorgang.

Die Freiwilligkeit ist ebenfalls eingeschränkt, wenn die hoheitliche Stelle die Einwilligung zu einer Datenverarbeitung zur Voraussetzung für die Erbringung einer Leistung macht, die aufgrund eines rechtlichen Monopols nur sie erbringen darf.[199] Ein rechtliches Monopol der ID Austria liegt nicht vor. Durch das System ausgelieferte Attribute haben zwar einen besonderen Stellenwert im Rechtsverkehr; ein rechtliches Monopol hinsichtlich dieser Verarbeitungstätigkeit liegt aber nicht vor.

[197] ErläutRV 469 BlgNR 27. GP 2.
[198] *Klement* in *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht (2019) Art 7 Rz 50.
[199] *Klement* in *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht (2019) Art 7 Rz 52.

Erstellung einer kryptografischen Bindung:

Die Erstellung einer kryptografischen Bindung stützt sich auf Art 6 lit e DSGVO. Die nationale Rechtsgrundlage ist § 4 Abs 5 E-GovG iVm § 2 Z 10a E-GovG mit der Maßgabe, dass die Zustimmung der Betroffenen vor der Erstellung der Bindung eingeholt wird. Bei dieser Zustimmung handelt es sich nicht um eine Einwilligung iSd Art 4 Z 11 DSGVO, da, wie erwähnt, die Verarbeitung auf Basis des Art 6 Abs 1 lit e DSGVO erfolgt. Vielmehr wird mit diesem zusätzlichen Schritt der „Zustimmung" das Recht auf informationelle Selbstbestimmung besonders betont, das heißt, dass die Freiwilligkeit im Vordergrund steht und erst nach dem initialen freiwilligen Handeln der Betroffenen die gesetzlichen Grundlagen anwendbar sind. Dass die Datenverarbeitung im gegenständlichen System zum Zweck der „Wahrnehmung einer Aufgabe [...], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt" (Art 6 Abs 1 lit e DSGVO) erforderlich ist und tatbestandsmäßig auf einer gesetzlichen Ermächtigung basiert, schließt nicht aus, dass die Verarbeitung grundsätzlich nur nach dem Willen der Betroffenen erfolgen soll. Die Erstellung einer kryptografischen Bindung ist eine spezifische Ausformung eines Verwendungsvorgangs des E-ID. Hier ist auf die oben angeführten Ausführungen der Materialien[200] zu verweisen.

4.2.5 Datenverarbeitung zum Zweck der Verwaltung des E-ID über „Meine ID Austria"

Betrieb der Applikation:

Der allgemeine Betrieb der Applikation und Website stützt sich auf Art 6 Abs 1 lit e DSGVO.

Einsicht in Transaktions-Logs:

Die Verarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO, sowie auf die nationale Bestimmung des § 18 Abs 1 E-GovG.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[201] aus:

„Wie bisher ist im Rahmen des E-ID-Systems sicherzustellen, dass die Protokollierung der Datenübermittlung aus dem E-ID-System im Auftrag des E-ID-Inhabers lediglich dem jeweiligen Betroffenen zugänglich ist. Die Protokollierung soll jedoch im Einklang mit den datenschutzrechtlichen Vorgaben der DSGVO auch für den Verantwortlichen und dessen Auftragsverarbeiter ersichtlich sein, da diese nur auf diesem Wege etwaigen Auskunfts- oder Löschungsersuchen der Betroffenen nachkommen können. Durch die Einfügung der Wortfolge „unbeschadet der datenschutzrechtlichen Verpflichtungen des Verantwortlichen und seiner Auftragsverarbeiter" soll daher klargestellt werden, dass den Betroffenenrechten und den Grundsätzen für die Verarbeitung von personenbezogenen Daten gemäß DSGVO unzweifelhaft nachgekommen und damit den datenschutzrechtlichen Verpflichtungen als Verantwortlicher erfüllt werden kann."

[200] ErläutRV 469 BlgNR 27. GP 7; ErläutRV 469 BlgNR 27. GP 2.
[201] ErläutRV 469 BlgNR 27. GP 7.

Zudem ist auf § 11 der (aktuell als Entwurf vorliegenden) Stammzahlenregisterbehördenverordnung 2022 zu verweisen, welcher derzeit lautet:[202]

„§ 11. Die Stammzahlenregisterbehörde hat in elektronischer Form allen Personen, deren eindeutige Identität durch die Verwendung des E-ID sichergestellt ist, die Anzeige einer Übersicht

1. über die von ihnen oder für sie gespeicherten Daten über das Bestehen von Vertretungsbefugnissen für die Vertretung von natürlichen Personen sowie

2. über die Protokolldaten der Datenübermittlung aus dem E-ID-System gemäß § 18 Abs. 1 E-GovG

zur Verfügung zu stellen."

Widerruf / Aussetzung des E-ID:

Die Verarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO. Die nationale Bestimmung ist hierbei § 4a Abs 5 E-GovG.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien aus:[203]

„Die Registrierung des E-ID erfolgt stets unter Verarbeitung personenbezogener Daten in der zentralen Evidenz, die Registrierungsdaten sind dem qualifizierten VDA zur Ausstellung eines qualifizierten Zertifikats zu übermitteln. E-ID-Inhaber haben das Recht, zu jedem Zeitpunkt eine vorübergehende Aussetzung sowie einen Widerruf des E-ID bei der Behörde zu verlangen. § 4a Abs. 5 verpflichtet die Behörden zudem zur Aussetzung oder zum Widerruf eines E-ID, insbesondere, wenn sie Kenntnis vom Tod des E-ID-Inhabers oder einer drohenden Missbrauchsgefahr erlangen sowie für den Fall, dass Zweifel an der Identität des Betroffenen aufkommen. Eine Erfüllung dieser Aufgaben ist unmöglich, wenn die Daten aufgrund eines Widerspruchs des Betroffenen nicht verarbeitet werden dürfen. Den Behörden würde im Falle eines Widerspruchs jede Handlungsmöglichkeit entzogen, die missbräuchliche Verwendung – insbesondere auch die Verwendung eines E-ID mit einer zweifelhaften Identität – zu unterbinden.

Auch sonst ist es zu Beweiszwecken und zur Vermeidung allfälliger Amtshaftungsansprüche unumgänglich, dass das Bestehen eines gültigen E-ID und damit die Möglichkeit der Verwendung im Rechtsverkehr bzw. der Zeitpunkt einer Aussetzung oder eines Widerrufs von den Behörden nachvollzogen werden kann."

[202] Siehe Begutachtungsfassung der Stammzahlenregisterbehördenverordnung (StZRegBehV) 2022.
[203] ErläutRV 469 BlgNR 27. GP 4.

4.3 Rollenverteilung nach Maßgabe der DSGVO

4.3.1 Allgemeine Systematik der Rollenverteilung

Grundlegend festzuhalten ist, dass die Eruierung der jeweiligen datenschutzrechtlichen Rolle datenverarbeitender Akteur*innen immer anhand der einzelnen Verarbeitungstätigkeit vorzunehmen ist. Außerdem kennt nach *Hödl* die DSGVO keine „Mischformen" in der Rollenverteilung, weshalb in Bezug auf die jeweilige konkrete Verarbeitungstätigkeit, der *Verantwortliche* nicht zugleich die Rolle des *Auftragsverarbeiters*, eines *Dritten*, *Empfängers* oder der betroffenen Person einnehmen kann;[204] dies trifft vice versa auch auf alle anderen Rollen zu.

Die grundlegende Systematik der Rollenverteilung nach Maßgabe der DSGVO lässt wie folgt überblicksartig zusammenfassen:

An oberster Stelle der Verantwortungskette bestimmt und wacht der ***Verantwortliche*** **(oder die gemeinsam *Verantwortlichen*)** als „Herr der Daten"[205] über die Verarbeitung personenbezogener Daten natürlicher Personen (= betroffene Person), da diesem gem Art 4 Z 7 DSGVO die alleinige (oder ggf gemeinsam ausgeübte) Entscheidungsmacht über die Festlegung der Zwecke und (wesentlichen) Mittel der Verarbeitung zusteht.[206]

Sofern jedoch zwei oder mehr *Verantwortliche* gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, führt dies zur sogenannten „pluralistische[n] Kontrolle"[207] über die jeweilige Datenverarbeitungstätigkeit, und die gemeinsame Verantwortlichkeit nach Maßgabe von Art 26 DSGVO ist damit begründet. Infolgedessen haben die gemeinsam *Verantwortlichen* eine Vereinbarung gem Art 26 Abs 1 und 2 DSGVO zu treffen, welche auch als Joint-Controller-Vereinbarung[208] bezeichnet wird. Darin muss klar festgelegt werden, dass eine gemeinsame Verantwortlichkeit zwischen den betreffenden *Verantwortlichen* vorliegt, wie jeder der *Verantwortlichen* an der Entscheidung über die Zwecke und Mittel der gemeinsamen Verarbeitung mitwirkt und welcher *Verantwortliche* welche Verpflichtungen nach der DSGVO zu erfüllen hat.[209]

Das Wesentliche dieser Vereinbarung muss den Betroffenen gem Art 26 Abs 2 Satz 2 DSGVO zur Verfügung gestellt werden, wobei die Zurverfügungstellung jener Inhalte mit den datenschutzrechtlichen Informationen gem Art 13 oder 14 DSGVO am praktikabelsten ist.[210]

Aus Art 26 DSGVO kommt zwar nicht hervor, was unter dem „Wesentlichen der Vereinbarung" zu verstehen ist, jedoch sollten nach *Horn* folgende Angaben darin enthalten sein:

- Namen und Kontaktdaten aller *Verantwortlichen*[211]

---

[204] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 89.
[205] *Raschauer* in *Sydow*, Europäische Datenschutzgrundverordnung[2] Art 4 Rz 123.
[206] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 83 f.
[207] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 10, 22, 38 f; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 80.
[208] EuGH C-210/16 VbR 2018/109; *Gabauer/Knyrim*, Checkliste Prüfschema zur datenschutzrechtlichen Rollenverteilung, Dako 2019/8, 14 (15).
[209] *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[210] Vgl *Feiler/Forgó,* EU-DSGVO Art 26 Anm 3.
[211] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Bertermann* in *Ehmann/Selmayr,* DS-GVO[2] Art 26 Rz 12; *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG[2] Art 26 Rz 9.

- Zweck(e) der gemeinsamen Verarbeitung;
- Einflussnahme der jeweiligen *Verantwortlichen* bei der Entscheidung über Zwecke und Mittel;
- Funktionale Beschreibung der gemeinsamen Verarbeitung, Aufgaben und Funktionen der jeweiligen *Verantwortlichen* sowie Offenlegung, wer welche Daten zu welchem Zweck verarbeitet;
- Beziehungen und Abhängigkeiten der wahrgenommenen Funktionen und der gemeinsam *Verantwortlichen* zueinander einschließlich allfälliger Datenübermittlungen zwischen den *Verantwortlichen*;
- Zuweisung eines *Verantwortlichen* zu jeder einzelnen sich aus der DSGVO ergebenden Pflicht für *Verantwortliche*; das Augenmerk sollte dabei insb auf die Betroffenenrechte gerichtet werden;[212]
- gegebenenfalls Benennung eines *Verantwortlichen* als zentrale Anlaufstelle nach Art 26 Abs 1 S 3.[213]

An der jeweiligen Verarbeitung kann auch ein ***Auftragsverarbeiter*** mitwirken, der dem *Verantwortlichen* stets als „verlängerter Arm"[214] dient, da der *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO als rechtlich eigenständige und externe Organisation[215] Datenverarbeitungstätigkeiten lediglich „im Auftrag" des *Verantwortlichen* durchzuführen hat. Folglich kommt dem *Auftragsverarbeiter* grds keine Entscheidungsbefugnis hinsichtlich der Verarbeitungszwecke und (wesentlichen) -mittel zu.[216] Allerdings kann der *Verantwortliche* dem *Auftragsverarbeiter* bezüglich der Wahl von technischen und organisatorischen Mitteln einen Entscheidungsspielraum in der zwingend aufzusetzenden Auftragsverarbeitungsvereinbarung gem Art 28 Abs 3 DSGVO einräumen, wodurch hinsichtlich der Wahl der „Mittel der Verarbeitung" eine gewisse Flexibilität herrscht.[217] Jedoch liegt die Entscheidungskompetenz über die „wesentlichen Mittel" der Verarbeitung stets beim *Verantwortlichen*.[218]

Die dem *Verantwortlichen* oder *Auftragsverarbeiter* unterstellten Personen gelten grds als ihnen „zurechenbare Personen"[219], da sie idR nur als „Ausführungsorgan" für den *Verantwortlichen* oder *Auftragsverarbeiter* tätig sind.[220] Dies gilt jedoch nur solange sie sich an die Vorgaben bzw vorab festgelegten Zwecke und Mittel der Verarbeitung halten.

---

[212] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[213] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41.
[214] *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter - was ändert sich mit der DSGVO? ZTR 2017, 59 (59).
[215] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 30.
[216] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 94.
[217] *Hartung* in *Kühling/Buchner*, DS-GVO/BDSG² Art 4 Nr 7 Rz 13; *Feiler/Forgó*, EU-DSGVO Art 4 Anm 12; *Artikel-29-Datenschutzgruppe,* Stellungnahme 1/2010, 17.
[218] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 17 f.
[219] Vgl *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (136); *Hödl* in*Knyrim*, DatKomm Art 4 Rz 83 unter Verweis auf *Raschauer* in *Sydow,* Europäische Datenschutzgrundverordnung Art 4 Rz 125.
[220] *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT, 31 (38).

Zum ***Empfänger*** gem Art 4 Z 9 DSGVO zählt potentiell fast jede*r datenverarbeitende Akteur*in,[221] welche*r zumindest ein „gewisses Maß an Eigenständigkeit“[222] aufzuweisen hat und dem*der personenbezogene Daten innerhalb einer Verarbeitungstätigkeit lediglich offengelegt werden.

Ferner gibt es auch die Rolle des „außenstehenden“[223] ***Dritten***, dessen charakteristisches Merkmal die grundsätzlich vom *Verantwortlichen* abzuleitende Legitimation und Befugnis zur Verarbeitung der betreffenden personenbezogenen Daten ist. Im Hinblick auf die betreffende Datenverarbeitung fehlen diese allerdings[224], was in der eigenverantwortlichen Datenverarbeitung des *Dritten* resultiert und weshalb dieser idR auch bei Umgang mit denselben personenbezogenen Daten selbst zu einem *Verantwortlichen* mutiert.

Die Rolle der **betroffenen Person** lässt sich aus der Legaldefinition zum Begriff „personenbezogene Daten“ gem Art 4 Z 1 DSGVO klar ableiten, wonach es sich bei der betroffenen Person nur um eine natürliche Person handeln kann, die anhand der zu verarbeitenden Daten identifiziert oder identifizierbar ist.[225] Folglich kann jeder lebende[226] Mensch die Rolle der betroffenen Person einnehmen, unabhängig von einer spezifischen Voraussetzung iS eines bestimmten Alters oder Geisteszustands.[227]

Festzuhalten ist daher, dass sich der Schutz personenbezogener Daten nach Maßgabe der DSGVO grundsätzlich nur auf Daten von natürlichen Personen richtet, was auch mehrfach explizit aus dem Verordnungstext hervorgeht.[228] Darüber hinaus wurde im ErwGr 14 Satz 2 DSGVO weiters klargestellt, dass Daten, welche sich auf juristische Personen beziehen, grundsätzlich nicht vom Anwendungsbereich der DSGVO umfasst sind.[229]

Sofern sich jedoch der Firmenwortlaut einer juristischen Person aus den Namen von ein oder mehreren natürlichen Personen zusammensetzt, was bei Personengesellschaften in Österreich eine durchaus übliche Praxis ist, so können Daten, die sich auf diese juristische Person beziehen, sehr wohl vom sachlichen Anwendungsbereich gem Art 2 DSGVO erfasst sein.[230]

Generell besteht allerdings eine gewisse Diskrepanz bezüglich des Schutzes personenbezogener Daten von juristischen Personen nach dem österreichischen Datenschutzgesetz (DSG) und der DSGVO, denn der Schutzbereich des Grundrechts auf Datenschutz gem § 1 DSG erstreckt sich sowohl auf natürliche

---

[221] Explizit ausgenommen vom Empfängerbegriff gem Art 4 Z 9 Satz 2 DSGVO sind Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach Unionsrecht oder nationalen Recht des jeweiligen Mitgliedstaats möglicherweise personenbezogene Daten erhalten – im ErwGr 31 DSGVO werden hierzu folgende Behörden bsph angeführt: „Steuer- und Zollbehörde, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, (…).“

[222] Vgl *Petri* in *Simitis/Hornung/Spiecker*, Datenschutzrecht Art 4 Nr 9 Rz 3 – spricht von „gewisse organisatorisch-institutionelle Eigenständigkeit“; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 103.

[223] Vgl *Ernst* in *Paal/Pauly*, DS-GVO/BDSG[2] Art 4 Rz 59; *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (136).

[224] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 108 DSGVO.

[225] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 6*; Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT, 31 (35).

[226] Vgl ErwGr 27 und 158 Satz 1 DSGVO.

[227] *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT, 31 (35).

[228] Vgl gem Art 1 Abs 1-3, Art 4 Z 1 sowie ErwGr 14 Satz 1 DSGVO.

[229] ErwGr 14 Satz 2 DSGVO: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Namen, Rechtsform oder Kontaktdaten der juristischen Person.“

[230] Vgl *Feiler/Forgó*, EU-DSGVO Art 4 Anm 1 unter Verweis auf EuGH 9. 11. 2010, C-92/09 und C-93/09 - *Schecke*, Rz 53.

als auch juristische Personen.[231] Nach systematischer Interpretation erfasst der Begriff „betroffene Personen“ daher in den einfachgesetzlichen Bestimmungen des DSG auch juristische Personen.[232] Diesen kommt dadurch auch das Beschwerderecht an die nationale Datenschutzbehörde (DSB) gem § 24 DSG, das Auskunftsrecht gem § 44 DSG und das Recht auf Berichtigung und Löschung gem § 45 DSG zu.[233]

Zurückzuführen ist dies darauf, dass mit § 1 Abs 3 DSG (Verfassungsrang) ein Ausgestaltungsvorbehalt bezüglich des Rechts auf Auskunft, Löschung und Berichtigung normiert wurde, weshalb diese Rechte nur „nach Maßgabe gesetzlicher Bestimmungen“ gelten.[234] Somit darf die „Art und Weise der Geltendmachung“ dieser Rechte zwar einfachgesetzlich konkretisiert werden, eine generelle „inhaltliche Beschränkung“ durch eine einfachgesetzliche Bestimmung würde dem engen Spielraum des Ausgestaltungsvorbehaltes jedoch zuwiderlaufen.[235] Dies erscheint folglich im Hinblick auf das einfachgesetzliche Datenschutz-Anpassungsgesetz 2018 äußerst fragwürdig, da demnach juristische Personen nicht mehr vom Begriff „betroffene Personen“ erfasst sind,[236] weshalb hierbei die einfachgesetzliche Ausgestaltung des § 1 Abs 3 DSG weitgehend inhaltlich beschränkt wurde und daher eine Verfassungswidrigkeit begründen könnte.[237]

Abschließend hierzu kann daher festgehalten werden, dass eine juristische Person auf Unionsebene iSd DSGVO die Rolle der betroffenen Person grundsätzlich nicht erfüllen soll bzw kann, wodurch unionsrechtlich ein Schutz personenbezogener Daten von juristischen Personen nicht besteht. Nach der österreichischen Rechtslage gilt allerdings „[…] der grundrechtliche Schutz personenbezogener Daten für juristische Personen verfassungsgesetzlich weiter“[238], was wiederum bedeutet, dass einfachgesetzliche Regelungen, die nicht auf juristische Personen Bezug nehmen der verfassungsrechtlichen Vorgabe gem § 1 DSG widersprechen.[239]

---

[231] *Heißl* in *Knyrim*, DatKomm Art 2 Rz 21 unter Verweis auf VfSlg 12.228/1989; 19.673/2012; OGH 28.6.2000, 6 Ob 162/00t; *Eberhard* in *Korinek/Holoubek* et al § 1 DSG Rz 25; *Ennöckl*, Schutz der Privatsphäre 143.

[232] *Heißl* in *Knyrim*, DatKomm Art 2 Rz 23 unter Verweis auf *Schwaiger* in Jelinek/Schmidl/Spanberger, DSG § 4 Anm 1; *Khakzadeh*, Die verfassungskonforme Interpretation in der Judikatur des VfGH, ZÖR 2006 201; krit *Kneihs,* Wider die verfassungskonforme Interpretation, ZfV 2009, 354.

[233] *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG § 4 Anm 10; *Heißl* in *Knyrim*, DatKomm Art 2 Rz 24; *Heißl* in *Lachmayer/v.Lewinski* (Hrsg), Datenschutz, 37 (44).

[234] *Heißl* in *Lachmayer/v.Lewinski* (Hrsg), Datenschutz, 37 (38).

[235] *Heißl* in *Lachmayer/v.Lewinski* (Hrsg), Datenschutz, 37 (45) unter Verweis auf VfSlg 11.548/1987; VfSlg. 16.986/2003.

[236] *Heißl* in *Knyrim*, DatKomm Art 2 Rz 25 unter Verweis auf *Anderl/Hörlsberger/Müller*, ÖJZ 2018, 15; *Leissler*, ecolex 2017, 1224.

[237] Vgl *Heißl* in *Knyrim*, DatKomm Art 2 Rz 25 unter Verweis auf *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, DSG § 4 Anm 10.

[238] *Heißl* in *Lachmayer/v.Lewinski* (Hrsg), Datenschutz, 37 (42).

[239] *Heißl* in *Lachmayer/v.Lewinski* (Hrsg), Datenschutz, 37 (45); siehe *Hödl* in *Knyrim*, DatKomm Art 4 Rz 8 – wonach mit § 4 Abs 1 DSG (einfachgesetzliche Regelung) zwar versucht wurde klarzustellen, dass die DSGVO nur auf natürliche Personen Anwendung findet, jedoch könnte diese Lösung verfassungsrechtlich noch auf den Prüfstand gestellt werden, da damit die einfachgesetzliche Regelung nach § 4 Abs 1 DSG dem in Verfassungsrang stehenden § 1 DSG – Grundrecht auf Datenschutz – widerspricht.

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) *Verantwortlichen*

Basierend auf der bisherigen und maßgeblichen Rechtsprechung[240] des Europäischen Gerichtshofs (EuGH) zur schwierigen Rechtslage hinsichtlich der Qualifikation eines oder mehrerer verantwortlicher datenverarbeitender Akteur*innen als einzeln *Verantwortliche* gem Art 4 Z 7 DSGVO oder als gemeinsam *Verantwortliche* gem Art 26 DSGVO, können zusammengefasst folgende Kriterien festgehalten werden. Diese Kriterien sind sowohl für die Ermittlung des *Verantwortlichen* bzw eines einzelnen *Verantwortlichen* als auch für die Ermittlung von gemeinsam *Verantwortlichen* zweckdienlich und sollen daher als Hilfestellung zur Abgrenzung von einzeln oder gemeinsam *Verantwortlichen* beitragen.

- Der Begriff des *„Verantwortlichen"* ist weit auszulegen, um so einen wirksamen und umfassenden Schutz der betroffenen Personen zu erzielen.[241]
- Das Festlegen von Kriterien für die Verarbeitung von personenbezogenen Daten iSd Parametrierens zum Zweck der Erstellung von Statistiken kann als eine maßgebliche Beteiligung an der Entscheidung über die Zwecke und Mittel der Verarbeitung gewertet werden.[242]
- Gemeinsame Verantwortlichkeit setzt nicht voraus, dass sämtliche *Verantwortliche* für dieselbe Verarbeitungstätigkeit einen (gemeinsamen) Zugang zu den betreffenden personenbezogenen Daten haben müssen.[243]
- Im Umkehrschluss kann dies jedoch bedeuten, dass, sofern mehrere *Verantwortliche*, die gemeinsam personenbezogene Daten erheben bzw verarbeiten, darüber hinaus auch über einen gemeinsamen Zugang zu den betreffenden personenbezogenen Daten verfügen, die Qualifikation derer als gemeinsam *Verantwortliche* naheliegt.
- Das Bestehen einer gemeinsamen Verantwortlichkeit hat nicht zwangsläufig eine gleichwertige Verantwortlichkeit sämtlicher *Verantwortlichen* für dieselbe Verarbeitungstätigkeit zur Folge.[244] Daher kann die Verantwortlichkeit bestimmter *Verantwortlicher* in verschiedenen Phasen und in unterschiedlichem Ausmaß ausgeprägt sein, wodurch der Grad der Verantwortlichkeit variieren kann.[245] Dabei kann man von einer qualitativ differenzierten Verantwortlichkeit sprechen. Charakteristisch hierfür ist, je größer die (Entscheidungs-)Macht eines *Verantwortlichen* über die Zwecke und Mittel der Verarbeitung ist, desto mehr Verantwortung geht damit einher bzw desto höher ist der Grad seiner Verantwortlichkeit.
- Das Organisieren, Koordinieren bzw „Ermuntern" zur Datenverarbeitung eines anderen *Verantwortlichen* (B) kann als eine auf Eigeninteresse beruhende Einflussnahme auf die Entscheidung über die Zwecke und Mittel der betreffenden Datenverarbeitung jenes *Verantwortlichen* (B) gedeutet werden. Dadurch wirkt der*die einflussausübende Akteur*in (A)

[240] EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317; EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388; EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551; EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.
[241] EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317, Rz 34.
[242] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 36 ff, 39.
[243] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 38.
[244] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.
[245] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.

letztendlich an der Entscheidung über die Zwecke und Mittel der Verarbeitung faktisch mit, woraus eine gemeinsame Verantwortlichkeit resultieren kann.[246]

- Als wesentliches Indiz für das Vorliegen von gemeinsam *Verantwortlichen* kann das Kriterium des gemeinsamen Ziels einer Datenverarbeitung herangezogen werden, weshalb bereits eine „Interessensgleichrichtung" für gemeinsam *Verantwortliche* sprechen kann.[247]
- Für die Entscheidung über Zwecke und Mittel der Verarbeitung bedarf es keiner schriftlichen Anleitung oder Anweisung zur gemeinsamen Datenverarbeitung.[248]
- Eine gemeinsame Entscheidung über das Mittel der Verarbeitung (wie Social Plug-In[249]) kann darin liegen, dass ein *Verantwortlicher* ein solches technisches Verarbeitungsmittel zur Verarbeitung einsetzt, durch das der*die Anbieter*in des Mittels an derselben davon umfassten Verarbeitungstätigkeit partizipieren kann.[250]
- Die gemeinsame Entscheidung über den oder die Zwecke der Verarbeitung kann durch eine stillschweigende Einwilligung eines *Verantwortlichen* über die Verarbeitung von personenbezogenen Daten durch einen anderen *Verantwortlichen* resultieren, wenn dies dieselbe Verarbeitungstätigkeit betrifft.[251]
- Die Grenzen der Verantwortlichkeit von gemeinsam *Verantwortlichen* liegen darin, dass ein gemeinsam *Verantwortlicher* für die vor- oder nachgelagerten Vorgänge innerhalb einer Verarbeitungskette, für die er weder die Zwecke noch die Mittel festgelegt hat, nicht als *Verantwortlicher* angesehen werden kann.[252]

4.3.3 Rollenverteilung im E-ID Gesamtsystem

Für die Rollenverteilung im E-ID Gesamtsystem, vor allem im Hinblick auf die Rolle des oder der *Verantwortlichen* kommt in Zusammenschau mit dem E-GovG zunächst der sogenannten „rechtlichen Verantwortlichkeit"[253] maßgebliche Bedeutung zu; dieser Beurteilungsaspekt geht aus Art 4 Z 7 2. Halbsatz DSGVO hervor. Demnach kann der *Verantwortliche* im Unionsrecht oder dem Recht der Mitgliedstaaten nach bestimmten Kriterien vorgesehen werden, sofern die Zwecke und Mittel der Verarbeitung durch das jeweilige Recht vorgegeben sind. So schlägt sich dieser Beurteilungsaspekt vor allem im öffentlichen Recht nieder, weshalb sowohl privaten als auch öffentlich-rechtlichen datenverarbeitenden Akteur*innen kraft nationalen Rechts einerseits bestimmte Aufgaben, die im öffentlichen Interesse liegen,[254] oder konkrete Verarbeitungstätigkeiten zugewiesen werden können.

[246] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 68, 70 ff.
[247] Vgl EuGH C-25/17 VbR 2018/110 (202).
[248] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 67.
[249] Social Plug-Ins können als Mittel der Verarbeitung angesehen werden, da durch deren Einbindung in Websites die Möglichkeit der Verarbeitung (Erhebung oder/und Übermittelung) von personenbezogenen Daten (auch durch Dritte) begründet wird -EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77.
[250] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77, 79.
[251] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 80 ff, 84.
[252] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 74, 85.
[253] *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110); *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG[2] Art 4 Nr 7 Rz 15.
[254] Vgl *Raschauer* in *Sydow,* Europäische Datenschutzgrundverordnung[2] Art 4 Rz 141; *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG[2] Art 4 Nr 7 Rz 14.

Daraus kann sich, basierend auf deren expliziter Zuständigkeit hierfür, ihre rechtliche Verantwortlichkeit betreffend der mit den zugewiesenen Aufgaben einhergehenden Verarbeitung von personenbezogenen Daten ergeben.

In Anbetracht des Beurteilungsaspekts der rechtlichen Verantwortlichkeit kommt vor allem § 4b Abs 1 E-GovG wesentliche Bedeutung zu, da demnach der Bundesminister für Inneres sowie die Bundesministerin für Digitalisierung und Wirtschaftsstandort in ihrer Funktion als Stammzahlenregisterbehörde (SZRB) ermächtigt sind all jene personenbezogenen Daten, die im Rahmen des E-ID-Registrierungsprozesses primär von den Registrierungsbehörden verarbeitet werden, zum Zweck der Verwaltung des E-ID Gesamtsystems zu verarbeiten.

Im Vergleich zum BMI ist an dieser Stelle jedoch die zentrale Rolle der SZRB bzw der BMDW im E-ID Gesamtsystem ua unter Verweis auf § 7 Abs 2 E-GovG hervorzuheben, aus dem hervorgeht, dass sich die SZRB „(...) bei der Führung des Ergänzungsregisters sowie bei der Errechnung von Stammzahlen und bei der Durchführung der in den §§ 4, 4b, 5, 9, 10, 14, 14a und 15 geregelten Verfahren des Bundesministeriums für Inneres als Auftragsverarbeiter, soweit natürliche Personen Betroffene sind, und des Bundesministeriums für Finanzen oder der Bundesanstalt Statistik Österreich hinsichtlich aller anderen Betroffenen bedienen“ kann.

Dabei handelt es sich bei den in §§ 4, 4b, 5, 9, 10, 14, 14a und 15 E-GovG geregelten Verfahren um systemimmanente Verfahren betreffend das E-ID Gesamtsystems, in denen nach dem Beurteilungsaspekt der rechtlichen Verantwortlichkeit zur Folge die SZRB/BMDW gegenüber etwaigen *Auftragsverarbeitern* stets als (rechtlich qualifizierter) *Verantwortlicher* auftritt.

Allerdings darf bei der Qualifikation des oder der *Verantwortlichen* nicht der funktionelle Aspekt außer Acht gelassen werden, denn dieser spiegelt das charakteristische Merkmal des *Verantwortlichen* wider und bezieht sich auf dessen maßgebliche „Entscheidungsfunktion“[255], zumal die vollumfängliche Verantwortung über eine Datenverarbeitung nur jene*r Akteur*in trägt, welche*r über die Zwecke und Mittel der Verarbeitung entscheidet.[256]

Hinsichtlich der Fähigkeit des Entscheidens ist daher für die Ermittlung des *Verantwortlichen* das „faktische Element“ besonders ausschlaggebend.[257] Demnach ist jene*r datenverarbeitende Akteur*in als *Verantwortlicher* zu qualifizieren, welche*r tatsächlich die Entscheidungsgewalt über die Verarbeitungszwecke und -mittel innehat bzw diese **de facto** ausübt.[258]

Um diese auf „[…] faktischen Elementen oder Umständen“ basierende Zuordnung der Rolle des *Verantwortlichen* zu erreichen,[259] sollte zunächst die jeweilige Verarbeitungstätigkeit isoliert betrachtet und ermittelt werden, um zu erfahren, warum diese Verarbeitung überhaupt durchgeführt wird.[260] Dies soll zur Extrahierung des konkreten Verarbeitungszwecks führen, woraus in weiterer Folge auch abgeleitet werden kann, wem die Verarbeitung der personenbezogenen Daten „dient“, um

[255] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83.
[256] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83; *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (101).
[257] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.
[258] *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (102); *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11 f.
[259] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.
[260] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.

in Zusammenschau mit sämtlichen Fakten die Schlüsselfrage „Wer hat sie veranlasst?“[261] praktikabel lösen zu können.

Daher ist bezüglich der Wertigkeit dieser beiden Beurteilungsaspekte festzuhalten, dass sich in der gesetzlich zugewiesenen Rolle des *Verantwortlichen* basierend auf der rechtlichen Verantwortlichkeit auch die faktische Entscheidungsmacht bzw „tatsächliche Kontrolle“[262] des betreffenden *Verantwortlichen* widerspiegeln muss.[263] Verarbeitet nämlich die ausdrücklich zuständige verantwortliche Stelle über ihre rechtliche Verantwortlichkeit hinaus personenbezogene Daten,[264] so verschiebt sich die Verantwortlichkeit basierend auf dem maßgeblichen „faktischen Ansatz“[265] zum*zur tatsächlich entscheidenden Akteur*in.[266]

4.3.3.1 Registrierung und Akkreditierung privater Service Provider

Basierend auf dem Beurteilungsaspekt der rechtlichen Verantwortlichkeit ist der BMI gem § 18 Abs 2 E-GovG der datenschutzrechtlich *Verantwortliche* gem Art 4 Z 7 DSGVO für die Verarbeitungstätigkeit der „Registrierung und Akkreditierung privater Service Provider“. Denn aus § 18 Abs 2 E-GovG geht explizit hervor, dass der BMI ermächtigt ist, *Dritten* iSd § 18 Abs 1 Z 3 E-GovG die Nutzung des E-ID Systems zu eröffnen. Im Konkreten handelt es sich bei der Eröffnung zur Nutzung des E-ID-Systems einerseits um die Registrierung von Service Ownern (SO) bzw Service Providern (SP). Andererseits umfasst die Verantwortlichkeit des BMI auch die Akkreditierung privater SP und deren Anwendungen.

Die rechtliche Verantwortlichkeit des BMI deckt sich dabei ebenso mit dem Beurteilungskriterium des „faktischen Ansatzes“, denn wie aus dem Kapitel 3.2.1 „Registrierung und Akkreditierung der Service Provider“ hervorgeht, erfolgt der Registrierungs- und Akkreditierungsprozess der Service Owner bzw Service Provider über das Service Provider-Register-Service (SPRS) des ID Austria Systems, für welches der BMI zuständig ist.

Im Auftrag des BMI fungiert hier das Bundesrechenzentrum (BRZ) als Dienstleister bzw im datenschutzrechtlichen Kontext als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, da es das SPRS zur Registrierung der Service Owner bzw Service Provider für den BMI zur Verfügung stellt.

4.3.3.2 Registrierung der Benutzer*innen

Aufgrund der Komplexität der Registrierung der Benutzer*innen im Hinblick auf die Rollenverteilung wird zunächst detailliert auf einschlägige Rechtsvorschriften für die Qualifikation des hierfür *Verantwortlichen* sowie auf die den betreffenden Verarbeitungsvorgängen zugrundeliegenden Verarbeitungszwecke eingegangen. Im Anschluss daran wird die Rollenverteilung für diese

[261] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.
[262] Vgl *EDPB* - Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, 11 Rz 23.
[263] Vgl *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 15.
[264] Worin *prima facie* eine unbefugte Verarbeitung liegt, da sie bspw nicht vom gesetzlich vorgegebenen Umfang der Verantwortlichkeit umfasst ist.
[265] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.
[266] Vgl *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110) unter Verweis auf *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 15.

Verarbeitungstätigkeit festgehalten, wobei die Verarbeitungstätigkeit „Registrierung von Benutzer*innen“ von der Erstellung der ID Austria differenziert abgehandelt wird.

Als *Verantwortliche* für die Verarbeitung personenbezogener Daten[267] im Rahmen der Registrierung des E-ID bzw der ID Austria sind im § 4b Abs 1 E-GovG „die mit der Registrierung des E-ID betrauten Behörden“ genannt. Hierbei erfolgt die Qualifikation des *Verantwortlichen* gem Art 4 Z 7 DSGVO primär nach der sogenannten „rechtlichen Verantwortlichkeit“.[268] Dabei sind sowohl die Zwecke als auch die (wesentlichen) Mittel der betreffenden Verarbeitung durch das E-GovG vorgegeben, da die verantwortlichen Registrierungsbehörden ermächtigt sind jene in § 4b Abs 1 und 3 sowie § 4a Abs 4 E-GovG normierten personenbezogenen Daten (iSd wesentlichen Mittel) zum Zweck der Registrierung des E-ID und zum Zweck der Überprüfung der Identität und der vorgelegten Dokumente innerhalb der Datenverarbeitung gem § 22b Passgesetz 1992, also innerhalb dem sogenannten Identitätsdokumentenregister (IDR), zu verarbeiten.

Mit der gesetzlich zugewiesenen Rolle des *Verantwortlichen* basierend auf der rechtlichen Verantwortlichkeit ist jedoch auch die faktische Entscheidungsmacht bzw -befugnis über die Datenverarbeitung zu den vorgegebenen Zwecken verbunden.[269] Daher ist Folgendes zu beachten: Verarbeitet die ausdrücklich zuständige verantwortliche Stelle über ihre rechtliche Verantwortlichkeit hinaus personenbezogene Daten,[270] so verschiebt sich die Verantwortlichkeit basierend auf dem maßgeblichen „faktischen Ansatz“[271] zum*zur tatsächlich entscheidenden Akteur*in.[272]

Zu jenen verantwortlichen Registrierungsbehörden zählen einerseits, hinsichtlich der Registrierung **von Amts wegen** (im Rahmen der Beantragung eines Reisedokuments, sofern die betroffene Person der Registrierung nicht widerspricht) die zuständige Passbehörde oder eine gem § 16 Abs 3 Passgesetz 1992 ermächtigte Gemeinde (sofern die Bezirksverwaltungsbehörde mit Zustimmung einer Gemeinde ihres Sprengels dies durch eine Verordnung bestimmt).

Andererseits zählen zu jenen verantwortlichen Registrierungsbehörden hinsichtlich der Registrierung des E-ID **auf Verlangen** der betroffenen Person neben der Passbehörde oder einer gem § 16 Abs 3 Passgesetz 1992 ermächtigten Gemeinde auch die LPD – Landespolizeidirektion und „andere geeignete Behörden“[273]. Dabei (Registrierung auf Verlangen) ist jene Behörde örtlich zuständig, bei der das Verlangen auf Registrierung seitens der betroffenen Person gestellt wurde.[274]

---

[267] Registrierungsdaten gem § 4b Abs 1 und Abs 3 E-GovG sowie das Lichtbild und der Abgleich jener Daten mit Registern von Verantwortlichen des öffentlichen Bereichs gem § 4a Abs 4 E-GovG.

[268] *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110); *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG[2] Art 4 Nr 7 Rz 15.

[269] Vgl *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 15.

[270] Worin prima facie eine unbefugte Verarbeitung liegt, da sie nicht vom gesetzlich oder vertraglich vorgegebenen Umfang der Verantwortlichkeit umfasst ist.

[271] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 11.

[272] Vgl *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110) unter Verweis auf *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 15.

[273] Gem § 4a Abs 1 E-GovG kann im Einvernehmen mit dem BMI die auf Verlangen der betroffenen Person beruhende Registrierung des E-ID auch bei solchen „andere[n] geeignete[n] Behörden“ vorgenommen werden, wobei hierzu der BMI solche Behörden im Internet zu veröffentlichen hat.

[274] In Anbetracht des sogenannten „personenbezogenen Aspekt[s]“, der festlegt, welche Entität als *Verantwortlicher* überhaupt agieren kann, kann auch eine solche Registrierungsbehörde als *Verantwortlicher* qualifiziert werden, da vom Begriff des „*Verantwortlichen“* gem Art 4 Z 7 DSGVO neben natürlichen und juristischen Personen, auch Behörden, Einrichtungen und andere Stellen umfasst sind. Vgl *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 1 ff; *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (100 f); *Hödl* in *Knyrim,* DatKomm Art 4 Rz 80.

Darüber hinaus ist gem § 4a Abs 2 E-GovG die jeweilige LPD örtlich (dort, wo der Antrag auf Registrierung gestellt wurde) sowie sachlich für die Registrierung des E-ID auf Verlangen eines „Fremden“ iSd § 2 Z 4 StbG, also von Personen, welche die österreichische Staatsbürgerschaft nicht besitzen, zuständig. Ferner kann auch hier die Registrierung des E-ID für „Fremde“ im Einvernehmen mit dem BMI bei „(…) andere[n] geeignete[n] Behörden“ vorgenommen werden, wobei hierzu der BMI solche Behörden im Internet zu veröffentlichen hat.

Dahingehend kann als verantwortliche Registrierungsbehörde für die Registrierung eines E-ID für „Fremde“ jedenfalls die örtlich sowie sachlich zuständige LPD eruiert werden und ggf auch „andere[n] geeignete[n] Behörden“.

Somit kann festgehalten werden, dass die jeweilige Registrierungsbehörde (Passbehörde, ermächtigte Gemeinde, LPD oder „andere geeignete Behörde”) als *Verantwortlicher* die Registrierungsdaten gem § 4b Abs 1 Z 1 – 13 sowie Abs 3 und § 4a Abs 4 (bzgl Lichtbild) E-GovG der E-ID-Werber*innen zum Zweck der Registrierung des E-ID bzw der ID Austria verarbeitet.

Darüber hinaus verarbeitet die jeweilige Registrierungsbehörde jene Registrierungsdaten auch im Rahmen eines Datenabgleichs mit diversen Registern gem § 4a Abs 4 E-GovG zum Zweck der Registrierung bzw zum Zweck der Überprüfung der Identität und der Dokumente der E-ID-Werber*innen.

Die Stammzahlenregisterbehörde (SZRB) hat zum Zweck der Erstellung des E-ID bzw der ID Austria aufgrund der Identitätsdaten (jene gem § 4b Abs 1 Z 1-4 und 6) der E-ID-Werber*innen deren Stammzahl zu ermitteln, und diese in verschlüsselter Form an den VDA zu übermitteln. Hierbei ist anzumerken, dass die Erstellung der ID Austria neben der Registrierung der Benutzer*innen ein zentraler Bestandteil des gesamten E-ID-Registrierungsprozesses ist. Der VDA stellt daraufhin das qualifizierte Zertifikat, das mit der Personenbindung zum E-ID der E-ID-Werber*innen verbunden werden soll, für eine elektronische Signatur aus. Zusätzlich zur von der SZRB ermittelten und an den VDA übermittelten Stammzahl hat die SZRB dem VDA die personenbezogenen Daten gemäß § 4b Abs 1 Z 1-4, 7, 10 und 11 der E-ID-Werber*innen sowie eine allfällige Beschränkung der Gültigkeitsdauer des Zertifikats gemäß § 4a Abs 2 zu übermitteln. Der VDA übermittelt daraufhin der SZRB den Identitätscode des ausgestellten Zertifikats. Damit ist der E-ID-Registrierungsprozess endgültig abgeschlossen, wodurch die E-ID-Werber*innen zum *E-ID-Inhaber* wurden.

Im Folgenden wird der Verarbeitungsvorgang der Registrierung der Benutzer*innen getrennt von der damit einhergehenden Erstellung der ID Austria abgehandelt.

*Registrierung der Benutzer*innen:*

Die **jeweilige Registrierungsbehörde** gem § 4b E-GovG ist ***Verantwortlicher*** für die Registrierung der Benutzer*innen bzw ID-Werber*innen, wovon die Verarbeitung von Registrierungsdaten im IDR samt dem Datenabgleich mit Registern sowie der Identifizierungsprozess umfasst sind. Dies erfolgt über definierte, organisatorische Prozesse und technische Komponenten, welche allesamt in der Registration-Domain, die wiederum von dem BMI bereitgestellt wird, angesiedelt sind.

Für die jeweilige Registrierungsbehörde als *Verantwortlicher* wird gem § 22b Abs 1b Passgesetz 1992 der **BMI als gesetzlicher *Auftragsverarbeiter*** gem Art 4 Z 8 DSGVO für den Betrieb des IDR eingesetzt, welcher sodann auch die für die Registrierung der Benutzer*innen notwendige Registration-Domain bereitstellt. Für die Führung von Datenverarbeitungen gem § 22a und § 22b Passgesetz 1992 und damit für die Führung des IDR (Datenverarbeitung nach § 22b Passgesetz 1992) fungiert letztendlich das **BRZ** als gesetzlicher ***Auftragsverarbeiter*** gem § 16 Abs 6 Passgesetz 1992.

Innerhalb der Registrierung der Benutzer*innen bzw ID-Werber*innen, wofür die jeweilige Registrierungsbehörde verantwortlich ist und den BMI als *Auftragsverarbeiter* für den Betrieb des IDR einsetzt, wird hinsichtlich der **Registrierungsvariante A** „Vorregistrierung mit der Dokumentennummer über die App ‚Digitales Amt'"[275] der **VDA** als **gesetzlicher *Sub-Auftragsverarbeiter*** gem § 4a Abs 3 E-GovG tätig.

Erstellung der ID Austria:

Für die Erstellung der ID Austria ist gem § 4 Abs 4 E-GovG die Bundesministerin für Digitalisierung und Wirtschaftsstandort als **Stammzahlenregisterbehörde** (SZRB) ***Verantwortlicher*** gem Art 4 Z 7 DSGVO.

Dabei bedient sich die SZRB gem § 7 Abs 2 E-GovG SZRB des **Bundesministeriums für Inneres** als ***Auftragsverarbeiter*** gem Art 4 Z 8 DSGVO, denn zwischen dem BMDW als SZRB und hierbei *Verantwortlicher* und dem BMI als *Auftragsverarbeiter* wurde innerhalb eines Verwaltungsübereinkommens ua eine Auftragsverarbeitungsvereinbarung gem Art 28 DSGVO getroffen, welche den Betrieb des Stammzahlenregisters (SZR) sowie dessen Wartung, die laufende Weiterentwicklung der betreffenden Software und der Systeme, als auch die Errechnung der Stammzahlen zum Gegenstand hat. Somit betreibt im Auftrag der BMDW als SZRB und *Verantwortlicher* das BMI als *Auftragsverarbeiter* das SZR und ist zudem zuständig für die Errechnung der Stammzahl, welche im Rahmen des E-ID-Registrierungsprozesses für die Erstellung der ID Austria benötigt wird. Dies deckt sich mit der Architektur des ID Austria Systems und dem restlichen Verwaltungsübereinkommen, denn das SZR ist Teil der Backend-Domain und diese wird ebenso im Auftrag der BMDW als SZRB und *Verantwortlicher* vom BMI als *Auftragsverarbeiter* betrieben.

Darüber hinaus wurde innerhalb des betreffenden Verwaltungsübereinkommens auch eine Auftragsverarbeitungsvereinbarung getroffen, deren Gegenstand die Führung des ERnP (Ergänzungsregister für natürliche Personen) umfasst. Dabei bedient sich gem § 7 Abs 2 E-GovG die BMDW als SZRB und *Verantwortlicher* ebenso des BMI als *Auftragsverarbeiter*.

Das BMI ist daher innerhalb der Verarbeitungstätigkeit „Registrierung von Benutzer*innen" auch für die Erstellung der ID Austria als *Auftragsverarbeiter* zu qualifizieren.

Das BMI, welches im Rahmen der Erstellung der ID Austria *Auftragsverarbeiter* ist, bedient sich für den Systembetrieb des BRZ als Dienstleister bzw als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO. Dadurch ist das BRZ als *Sub-Auftragsverarbeiter* für die Erstellung der ID Austria zu qualifizieren.

[275] Siehe näheres hierzu in Kapitel 3.2.2.3 Registrierungsvarianten.

Das BRZ ist gem § 16 Abs 6 Passgesetz 1992 gesetzlicher *Auftragsverarbeiter* für die Führung des IDR, allerdings betrifft dies nur den Teilaspekt der „reinen" Registrierung der Benutzer*innen. Davon nicht betroffen ist die Erstellung der ID Austria, da diese auch nicht im oder durch das IDR erfolgt, sondern durch die Stammzahlenregisterbehörde (BMDW), wobei das BMDW zur Führung des Stammzahlenregisters wiederum das BMI als *Auftragsverarbeiter* nutzt. Sofern dies zutrifft, ist das BRZ hinsichtlich der Erstellung der ID Austria als *Auftragsverarbeiter* des BMI zu qualifizieren.

Neben der BMDW als SZRB und *Verantwortlicher* für die Erstellung der ID Austria ist hierbei der **VDA** als **alleiniger *Verantwortlicher*** gem Art 4 Z 7 DSGVO zu qualifizieren. Dieser wird nämlich innerhalb dieser Teil-Verarbeitungstätigkeit streng nach Maßgabe der gesetzlichen Vorgaben hinsichtlich der Zwecke und wesentlichen Mittel der betreffenden Verarbeitung gem § 4 Abs 4 E-GovG im eigenen Namen für die betroffene Person bzw ID-Werber*in tätig, um im Rahmen der Erstellung der ID Austria für diese*n die Zertifikatsbindung qcBind zur Authentifizierung zu erstellen.

Eine gemeinsame Verantwortlichkeit zwischen dem VDA und der SZRB kann hierbei nicht eruiert werden, solange der VDA für diesen Vorgang innerhalb der betreffenden Verarbeitungstätigkeit ausschließlich nach Maßgabe der einschlägigen nationalen und unionsrechtlichen Rechtsvorschriften iSd E-GovG, SVG und eIDAS-VO tätig wird, keine darüber hinausgehenden Zwecke oder wesentlichen Mittel der Verarbeitung gemeinsam mit der SZRB festlegt und keine über die rechtlichen Vorgaben hinausgehende Verarbeitungen personenbezogenen Daten mit der SZRB vornimmt.

Zur Umsetzung der Push-Benachrichtigungen an Android-Endgeräten bedient sich der jeweilige Verantwortliche zudem des durch Google Inc. betriebenen Zusatzdienstes „Firebase Cloud Messaging". Um den Versand von Push-Benachrichtigungen zu ermöglichen, wird beim Erst-Start der App ein „Firebase Cloud Messaging Registration-Token" erstellt, welcher die App-Installation auf dem Gerät eindeutig identifiziert. Diese Verarbeitung finden zusätzlich zu den allgemeinen Verarbeitungen des Android-Betriebssystems statt. Der im Rahmen der Nutzung von Google Firebase eingegangene Vertrag[276] definiert die **Google Inc. als *Auftragsverarbeiter***. Da es sich um einen optionalen Zusatzdienst handelt, welcher über die allgemeine Geräteinfrastruktur hinausgeht, liegt auch faktisch ein Auftragsverarbeitungsverhältnis vor.

Die Umsetzung der Push-Benachrichtigungen an Apple-Endgeräten erfolgt über das Apple Notification Service. Diese Verarbeitungstätigkeit wird im Zuge der allgemeinen Betriebssystemkommunikation abgewickelt. Die Applikation ruft in dieser Hinsicht keine zusätzlichen Verarbeitungen personenbezogener Daten hervor. Deshalb liegt aus Sicht der jeweiligen Verantwortlichen keine Auftragsverarbeitung durch Apple Inc. vor.

4.3.3.3 Verwendung des E-ID

Für die Verarbeitungstätigkeit „Verwendung des E-ID zur Nutzung von Anwendungen" iSd Anmeldung bei einer Datenverarbeitung (Anmeldung an Service Provider) sowie für die Bindingerstellung

[276] Siehe https://firebase.google.com/terms/data-processing-terms (abgerufen am 22.04.2022)

(Zertifikatsbindung bcBind sowie eIDASBind) ist die Bundesministerin für Digitalisierung und Wirtschaftsstandort als **Stammzahlenregisterbehörde** (SZRB) *Verantwortlicher* gem Art 4 Z 7 DSGVO.

Dabei bedient sich die SZRB gem § 7 Abs 2 E-GovG des **BRZ** als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, denn das BRZ betreibt im Auftrag der SZRB die **Frontend-Domain**, welche notwendige Funktionalitäten zur Authentifizierung von Benutzer*innen im Zuge von Anmeldeprozessen an Services und Applikationen, die über eine Anbindung zum ID Austria System verfügen, implementiert. Darin sind die verschiedenen Funktionalitäten durch technische Komponenten wie zB den Shibboleth Indentity Provider (IDP) zur Authentifizierung des *E-ID-Inhabers* und die Aggregation aller notwendigen Identitätsattribute oder das Binding Service zur vereinfachten, wiederholten Authentifizierung (Zertifikatsbindung bcBind) realisiert.

Im Rahmen dieser Verarbeitungstätigkeit bedient sich die SZRB gem § 7 Abs 2 E-GovG auch des **BMI** als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, denn zwischen der BMDW als SZRB und hierbei *Verantwortlicher* und dem BMI als *Auftragsverarbeiter* wurde innerhalb eines Verwaltungsübereinkommens ua eine Auftragsverarbeitungsvereinbarung gem Art 28 DSGVO getroffen, dessen Gegenstand den Betrieb des **E-ID Backend** umfasst. Konkret umfasst dieses Auftragsverarbeitungsverhältnis den Betrieb des Applikationsregisters für Anwendungen des öffentlichen Bereichs,[277] die Anforderung der Personenbindung aus dem SZR, die Abholung weiterer Merkmale aus angebundenen Registern und die Einfügung dieser Merkmale in die Personenbindung. Ferner gehört zu den Aufgaben des BMI als *Auftragsverarbeiter* die Beratung zu Webservices der Schnittstelle, die Erstellung von Statistiken, Monats- und Jahresberichten, die Teilnahme an Jour fixes mit der Stammzahlenregisterbehörde, die stichprobenartige Überprüfung der Berechtigung im Onlinebereich, eine laufende Anpassung der Dokumentation, die Erfassung der von Kunden gemeldete Fehler und Überwachung der Behebung, die Konzeption und Use-Case Erstellung für mögliche Erweiterungen, die Unterstützung bei der Zertifikats- und Berechtigungsverwaltung sowie die Testunterstützung für neue Releases etc.

Darüber hinaus wurde innerhalb des betreffenden Verwaltungsübereinkommens auch eine Auftragsverarbeitungsvereinbarung getroffen, dessen Gegenstand den Betrieb des **eIDAS-Knoten** umfasst. Dabei bedient sich die BMDW als SZRB und *Verantwortlicher* ebenso des BMI als *Auftragsverarbeiter*.

Das BMI ist daher innerhalb der Verarbeitungstätigkeit „Verwendung des E-ID zur Nutzung von Anwendungen“ einerseits hinsichtlich der Anmeldung bei einer Datenverarbeitung (Anmeldung an Service Provider) als Betreiber der Backend-Domain, der Register-Domain sowie der Attribut Provider-Domain, als Auftragsverarbeiter gem Art 4 Z 8 DSGVO zu qualifizieren.

Ebenso ist das BMI als Betreiber der eIDAS-Domain innerhalb der Verarbeitungstätigkeit „Verwendung des E-ID zur Nutzung von Anwendungen“ hinsichtlich der Zertifikatsbindung eIDAS-Bind zur Authentifizierung von Bürger*innen anderer EU-Mitgliedsstaaten, als Auftragsverarbeiter gem Art 4 Z 8 DSGVO zu qualifizieren.

[277] Das BMI ist *Verantwortlicher* für die Daten der privaten Service Provider. Zu öffentlichen Service Providern gibt es keine personenbezogenen Daten. Für den Betrieb des gesamten App-Register (öffentlicher und privater Bereich) setzt das BMI das BRZ als Dienstleister ein.

Hinsichtlich der Binding-Erstellung betreffend der **Zertifikatsbindung qcBind** bleibt der **VDA** alleiniger *Verantwortlicher* gem Art 4 Z 7 DSGVO für die fortlaufende Authentifizierung über ihn selbst. Dies jedoch nur solange die Benutzer*innen nicht die Zertifikatsbindung bcBind zur vereinfachten Authentifizierung über den zentralen Identity Provider[278] des ID Austria Systems erstellt haben.

Teil der Verarbeitungstätigkeit „Verwendung des E-ID zur Nutzung von Anwendungen“ ist auch die **Signaturerstellung**, denn die Benutzer*innen (als *ID-Inhaber*) können die ID Austria bzw das damit verknüpfte Zertifikat zur Erstellung einer qualifizierten Signatur (zB PDF-Signatur) anwenden. Dabei wird das qualifizierte Zertifikat (bzw der mit diesem Zertifikat verknüpfte private Signaturschlüssel) zentral durch den VDA verwaltet. Zur Erstellung einer qualifizierten Signatur authentifizieren sich die Benutzer*innen mit den für ihre ID Austria registrierten Authentifizierungsfaktoren beim VDA, woraufhin dieser die Signatur für die Benutzer*innen erstellt.

Somit ist für diese Teil-Verarbeitungstätigkeit iSd reinen Signaturerstellung der **VDA** als alleiniger *Verantwortlicher* gem Art 4 Z 7 DSGVO zu qualifizieren, da dieser streng nach Maßgabe der einschlägigen nationalen und unionsrechtlichen Rechtsvorschriften iSd SVG und eIDAS-VO hinsichtlich der Zwecke und wesentlichen Mittel der betreffenden Verarbeitung im eigenen Namen für die betroffene Person bzw Benutzer*in tätig wird.

Zur Umsetzung der Push-Benachrichtigungen an Android-Endgeräten bedient sich der jeweilige Verantwortliche des durch Google betriebenen Zusatzdienstes „Firebase Cloud Messaging“. Das Unternehmen Google Inc. ist daher auch in diesem Verarbeitungsprozess als Auftragsverarbeiter iSv Art 4 Z 8 DSGVO zu qualifizieren.[279]

4.3.3.4 Verwaltung des E-ID über „Meine ID Austria“

Innerhalb der Verarbeitungstätigkeit „Meine ID Austria“ ist für den **Widerruf des E-ID bzw der ID Austria** der **VDA** als alleiniger *Verantwortlicher* gem Art 4 Z 7 DSGVO zu qualifizieren. Dieser wird nämlich innerhalb dieser Teil-Verarbeitungstätigkeit nach Maßgabe der einschlägigen nationalen und unionsrechtlichen Rechtsvorschriften hinsichtlich der Zwecke und wesentlichen Mittel der betreffenden Verarbeitung gem § 4a Abs 5 E-GovG sowie § 6 SVG bzw Art 24 Abs 3 eIDAS-VO einerseits für die betroffene Person (*ID-Inhaber*) tätig, um auf deren Verlangen die Aussetzung oder den Widerruf des E-ID bzw der ID Austria (also die Aussetzung oder den Widerruf des mit der ID Austria verbundenen qualifizierten Zertifikats) zu bewirken. Zudem wird der VDA als *Verantwortlicher* nach Maßgabe der einschlägigen nationalen und unionsrechtlichen Rechtsvorschriften hinsichtlich der Zwecke und wesentlichen Mittel der betreffenden Verarbeitung gem § 4a Abs 5 E-GovG sowie § 6 SVG bzw Art 24 Abs 3 eIDAS-VO von sich aus oder veranlasst von der jeweils zuständigen Registrierungsbehörde für die betroffene Person tätig, um die Aussetzung oder den Widerruf der ID Austria zu bewirken, wenn bspw bekannt wird, dass der *ID-Inhaber* verstorben ist, die Gefahr missbräuchlicher Verwendung droht, oder den Behörden Tatsachen bekannt werden, die berechtigte Zweifel an der Identität der betroffenen Person bzw des *ID-Inhabers* aufkommen lassen.

[278] Dafür ist nämlich die SZRB verantwortlich, als *Verantwortlicher* der Frontend-Domain, welche wiederum vom BRZ auftragsgemäß betrieben wird.
[279] Siehe 4.3.3.2.

4.4 Angaben über Maßnahmen zur Einhaltung der DSGVO

4.4.1 Grundsatz der Zweckbindung

Die Zweckbindung von Datenverarbeitungen ist ein fundamentaler Grundsatz des Datenschutzrechts und konkret in Art 5 Abs 1 lit b DSGVO verankert.[280] Der *Verantwortliche* hat demnach **im Vorhinein** die Zwecke der Verarbeitung festzulegen und darf nur in bestimmten Ausnahmefällen davon abweichen. Dem liegt der Gedanke zugrunde, dass eine betroffene Person nur dann im Sinne ihrer informationellen Selbstbestimmung handeln kann, wenn sie von vornherein Kenntnis von den Zwecken der Verarbeitung ihrer Daten erlangen kann.[281]

§ 2 Z 10 E-GovG definiert den E-ID als eine „logische Einheit", die eine qualifizierte elektronische Signatur mit einer Personenbindung und den zugehörigen Sicherheitsdaten und -funktionen verbindet. Gem § 4 Abs 1 E-GovG dient der E-ID „[…] dem Nachweis der eindeutigen Identität, weiterer Merkmale sowie des Bestehens einer Einzelvertretungsbefugnis […] und der Authentizität des elektronisch gestellten Anbringens in Verfahren […]."

Um die Funktion des E-ID nutzen zu können, bedarf es gem § 4 Abs 3 E-GovG einer vorherigen Registrierung der E-ID-Werber*innen und einer damit einhergehenden Verarbeitung personenbezogener Daten. Dies gilt in weiterer Folge auch für die eigentliche Verwendung bzw Nutzung des E-ID.[282]

Über den Prozess der Registrierung werden die interessierten Personen zu *E-ID-Inhabern* und können das ID Austria System nutzen. Dabei werden für die Erstellung und Nutzung des E-ID erforderliche Daten der E-ID-Werber*innen erhoben, geprüft und – sofern notwendig – hinterlegt. Nach dem erfolgreichen Abschluss dieser Registrierung steht den Bürger*innen der persönliche E-ID zur Verwendung zur Verfügung.

Innerhalb dieses Prozesses ist zwischen der eigentlichen Registrierung der Benutzer*innen und der dann erfolgenden Erstellung der ID Austria zu differenzieren. Dabei umfasst die Registrierung der Benutzer*innen die Identitätsfeststellung bei der jeweiligen Registrierungsbehörde sowie die Verarbeitung von Registrierungsdaten im IDR samt einem Abgleich mit einschlägigen Registern. Die Abfrage der Register erfolgt zur Identitätsüberprüfung und soll zudem zur Qualitätssicherung der Daten dienen, weil dadurch nicht kongruente Registerdatensätze richtiggestellt werden können. Der Verarbeitungszweck der Erstellung der ID Austria umfasst hingegen die Generierung des E-ID nach Maßgabe von § 4 Abs 4 E-GovG. Dabei erfolgt die Ermittlung der SZ der E-ID Werber*innen durch die Stammzahlenregisterbehörde. Die SZ wird in verschlüsselter Form an den VDA übermittelt. Dieser stellt das qualifizierte Zertifikat für eine elektronische Signatur aus, das mit der Personenbindung zum E-ID der E-ID Werber*innen verbunden werden soll. Zudem hat die SZRB dem VDA die personenbezogenen Daten der E-ID-Werber*innen gemäß § 4b Z 1 bis 4, 7, 10 und 11 E-GovG sowie

[280] Siehe zudem die primärrechtliche Grundlage in Art 8 Abs 2 EU-Grundrechte-Charta (GRC).
[281] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DSGVO (2018) 37.
[282] Siehe hierzu die Ausführungen in §§ 4 ff E-GovG.

eine allfällige Beschränkung der Gültigkeitsdauer der Zertifikate gemäß § 4a Abs 2 E-GovG zu übermitteln.

Wesentlicher Zweck der E-ID ist somit die Authentifizierung der *E-ID-Inhaber* gegenüber dem zentralen Identitätsprovider des E-ID Systems im Zuge der Anmeldung an einen Service Provider und die Erstellung von Signaturen bzw Bindings. Dabei wird der E-ID und das damit verbundene Zertifikat zur Erstellung einer qualifizierten elektronischen Signatur verwendet. Die Authentifizierung erfolgt grundsätzlich über den VDA, der das qualifizierte Zertifikat zentral verwaltet. Durch die Erstellung der kryptographischen Bindung wird es dem *E-ID Inhaber* wiederum ermöglicht, die Personenbindung auch mittels eines sicherheitstechnisch gleichwertigen Vorgangs, der an eine frühere qualifizierte elektronische Signatur des *E-ID-Inhabers* gebunden ist, auszulösen.

In Zukunft sollen hierbei auch über die Kernidentitätsdaten hinausgehende Attribute aus Registern von *Verantwortlichen* des privaten und (wie bisher) öffentlichen Bereichs, die der SZRB zugänglich sind, im Auftrag des *E-ID-Inhabers* an *Dritte* übermittelt werden können.[283]

Weiters ist die Zweckbindung vor allem im Zusammenhang mit der Einbindung der Service Owner bzw Provider und deren Anwendungen von Bedeutung. Der Grundsatz der Zweckbindung kommt dabei über § 18 Abs 2 letzter Satz E-GovG zum Ausdruck:

„Die gemäß Abs. 1 [Anm § 18 E-GovG] übermittelten personenbezogenen Daten dürfen im konkreten Fall nur für die glaubhaft gemachten eigenen Zwecke verarbeitet werden; die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck im Sinne dieser Bestimmung."

Damit soll eine missbräuchliche Datenverwendung oder ungenügende Maßnahmen zur Datensicherheit verhindert bzw unterbunden werden, wobei die genauen Vorgaben durch Verordnungen des BMI geregelt werden.[284]

4.4.2 Grundsatz der Datenminimierung

Ein weiterer zentraler Grundsatz des Datenschutzrechts ist jener der Datenminimierung gem Art 5 Abs 1 lit c DSGVO. Die verarbeiteten personenbezogenen Daten sollten demnach für die Zwecke, zu denen sie verarbeitet werden, angemessen, erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[285] Zudem haben *Verantwortliche* gem Art 25 DSGVO die Pflicht, die Datenminimierung durch Technikgestaltung und datenschutzfreundliche Voreinstellungen wirksam umzusetzen.

In praktischer Hinsicht heißt dies vor allem, dass die Risiken schon durch die Gestaltung der Architektur des Systems so gering wie möglich zu halten sind. Wenn sich aufgrund des Zwecks der Verarbeitung bspw nicht erklären lässt, warum personenbezogene Daten besser zentral als nur auf dem Endgerät gespeichert werden sollen, dann kann nur eine lokale Datenhaltung rechtmäßig sein. Wenn eine allenfalls unvermeidbare zentrale Datenhaltung auch mit einer Pseudonymisierung (Verschlüsselung)

[283] Vgl ErläutRV 469 BlgNR 27. GP 2.
[284] Vgl ErläutIA 2227/A BlgNR 25. GP 15; siehe § 18 Abs 3 E-GovG.
[285] Siehe auch ErwGr 39 DSGVO.

umgesetzt werden kann, dann ist eine unverschlüsselte Datenhaltung nicht rechtmäßig. Wenn eine längere Löschfrist das Risiko für die Benutzer*innen erhöht, ist die Frist für jeden Anwendungsfall so kurz wie nötig zu wählen.

Dass die Entwicklung solcher Ansätze höhere Kosten bringt, ist streng genommen nur bei bestehenden („legacy“) Systemen beachtlich. Der *Verantwortliche* muss nämlich vom ersten Moment an auf Basis dieser Vorgaben Entscheidungen treffen. Tatsächlich kostspielig ist dies nur, wenn die Entwicklung bereits ohne deren Beachtung begonnen hat und erst später Entscheidungen getroffen werden, die wesentliche Auswirkungen auf die Architektur der Datenhaltung haben. Die Pflichten nach Art 25 („Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“) und Art 35 („Datenschutz-Folgenabschätzung“) DSGVO sind ebenso wie die Haftungsbestimmungen der DSGVO nicht offen gegenüber einer Argumentation mit zu hohen Entwicklungskosten.[286]

Der Grundsatz der Datenminimierung und das Prinzip „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ gem Art 25 DSGVO („Privacy by Design“) wurde in der Gestaltung der Anwendung sowie der dahinterliegenden Datenbank von vornherein berücksichtigt. Dies äußert sich wie folgt:

- Bereits die Architektur des ID Austria Systems folgt dem „Privacy by Design“ Prinzip des Datenschutzrechts und damit auch dem Grundsatz der Datenminimierung;
- Die Protokollierung ist hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt;
- Personenbezogene Daten unterliegen stringenten Pseudonymisierungs- und Löschfristen;
- Personenbezogene Daten werden nur von jenen Stellen verarbeitet bzw übermittelt, soweit diese hierfür notwendig sind;
- Gespeicherte personenbezogene Daten unterliegen strengen Zugriffsrechten;
- Es werden nur die für die Zweckerfüllung erforderliche Daten erhoben bzw sind im Registrierungs- und Anmeldeprozess nur Felder und Funktionen vorgesehen, die erforderlich sind.

Konkret wird der Grundsatz der Datenminimierung im Rahmen des ID Austria Systems bspw umgesetzt, indem ausschließlich eine selektive Übermittlung von Personenmerkmalen an Service Provider, welche über die entsprechende Berechtigung verfügen, stattfindet. Diese Berechtigungen werden im Zuge der Registrierung des Service Providers am ID Austria System sorgfältig geprüft und erteilt. Bei jedem Anmeldeprozess können Benutzer*innen zudem die an den Service Provider zu übermittelten Daten einsehen und müssen der Übermittlung zustimmen. Einen besonderen Schutz erfährt bei der ID Austria die Stammzahl von Bürger*innen, die als Basis für die Berechnung der zum Einsatz kommenden sektorspezifischen Identifikatoren fungiert. Die ID Austria schützt die Stammzahl speziell, indem das zugrundeliegende Konzept vorsieht, dass diese die behördlichen Register zu keiner Zeit unverschlüsselt verlässt. Der Schutz der Identitätsmerkmale (Attribute) von Bürger*innen ist ein

[286] Siehe hierzu weiterführend *Hötzendorfer*, Zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung. In: *Hötzendorfer*/*Tschohl*/*Kummer* (Hrsg): International Trends in Legal Informatics, Festschrift for Erich Schweighofer, Editions Weblaw, Bern, 2020, 419–437, 435.

zentrales Design-Prinzip der ID Austria. Die selektive, benutzerkontrollierte Übermittlung von Attributen an Service Provider und der spezielle Schutz der Vertraulichkeit der Stammzahl sind zwei der wichtigsten Maßnahmen, um diesem Design-Prinzip gerecht zu werden.

4.4.3 Grundsatz der Speicherbegrenzung

Zudem ist für die vorliegende DSFA noch der Grundsatz der Speicherbegrenzung gem Art 5 Abs 1 lit e DSGVO relevant. Demnach dürfen personenbezogene Daten nur so lange verarbeitet werden, wie es für die Zweckerreichung erforderlich ist oder eine gesetzliche Verpflichtung zur Aufbewahrung oder Archivierung besteht.

Einschlägige Informationen zur Speicherdauer von Daten finden sich bspw in der Datenschutzinformation des *Verantwortlichen*.[287] So wird dort darüber informiert, dass die Zugriffe der Nutzer*innen auf das ID Austria System zur Überprüfung der Systemsicherheit und Fehleranalyse sowie zu statistischen Zwecken für einen Zeitraum von sechs Monaten in einer Protokolldatei (Serverlogs) gespeichert werden.[288]

Hinsichtlich der Daten der Service Owner bzw Provider (sog *Dritter* gem § 18 Abs 1 Z 3 E-GovG) wird auf gesetzlicher Ebene in § 18 Abs 6 E-GovG festgelegt, dass diese dann zu löschen sind, wenn das E-ID System durch die Service Owner bzw Provider über einen Zeitraum von fünf Jahre nicht genutzt wurde. Die Gesetzesmaterialien führen als Hintergrund hierzu aus, dass nach diesem Zeitraum vermutlich regelmäßig davon ausgegangen werden kann, dass der *Dritte* nicht mehr an einer entsprechenden Benutzung des Systems interessiert ist.[289]

In Hinblick auf die Registrierung der Nutzer*innen sieht § 4b Abs 5 E-GovG wiederum vor, dass die dabei bekanntgegebenen Zustelladressen zu löschen ist, sobald die Registrierung des E-ID abgeschlossen wurde. Die Gesetzesmaterialien führen zudem wie folgt aus: „Die Löschungsregelung in Abs. 5 [Anm § 4b Abs 5 E-GovG] wird vor dem Hintergrund des datenschutzrechtlichen Grundsatzes der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit e DSGVO vorgeschlagen: Die bekanntgegebene Zustelladresse wird beispielsweise nur bis zum vollständigen Abschluss der Registrierung des E-ID benötigt, insbesondere um dem Betroffenen die Zugangsdaten zum E-ID zu übermitteln.“ [290]

Weiters sind Identitätscodes der ausgestellten Zertifikate gem § 4b Abs 5 E-GovG im Falle eines Widerrufs oder Ablaufs des jeweiligen Zertifikats zu löschen. Die Gesetzesmaterialien führen hierzu aus, dass „[s]obald ein Betroffener sein E-ID-Zertifikat widerruft oder das E-ID-Zertifikat abläuft, […] auch kein Grund mehr für die Aufbewahrung des zugehörigen Identitätscodes [besteht].“[291]

Darüber hinaus sind gem § 4b Abs 5 letzter Satz E-GovG auch alle sonstigen gem § 4b Abs 1 und 3 leg cit sowie § 4a Abs 4 verarbeiteten Daten zu löschen, sobald diese nicht mehr benötigt werden, spätestens jedoch drei Jahre nach dem Ablauf oder Widerruf des E-ID. Die Gesetzesmaterialien stellen hierzu Folgendes klar:

[287] https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22.04.2022).
[288] https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22.04.2022).
[289] ErläutRV 469 BlgNR 27. GP 9.
[290] ErläutRV 469 BlgNR 27. GP 6.
[291] ErläutRV 469 BlgNR 27. GP 6.

„Diese Regelung soll die Registrierung von Betroffenen, die sich erneut für einen E-ID entscheiden, dahingehend erleichtern, dass die eindeutige Identitätsfeststellung im Sinne des § 4a Abs. 4 durch die Registrierungsbehörde unter Verwendung der bereits in der zentralen Evidenz verarbeiteten Daten (insbesondere auch des Lichtbilds) erfolgen kann. Dadurch kann eine wesentliche Verwaltungserleichterung erzielt werden und können die Betroffenen von einer raschen und unkomplizierten Registrierung des E-ID profitieren. Die Aufbewahrung der personenbezogenen Daten ist zudem im Hinblick auf E-ID, die aufgrund von missbräuchlicher Verwendung oder zweifelhaften Identitäten widerrufen wurden, erforderlich. Diese Information muss für sämtliche Behörden verfügbar sein, um die erneute Registrierung eines E-ID in diesen Fällen zu vermeiden.“ [292]

Gem § 4a Abs 3 E-GovG können zudem bestimmte Daten,[293] die Inhaber*innen eines österreichischen Reisepasses den entsprechenden Behörden über den VDA zur Verfügung gestellt haben, um diese zum Zweck der E-ID-Registrierung weiterzuverarbeiten, 30 Tage speichern.[294] Diese Daten dienen im Wege der Vorregistrierung der Effizienzsteigerung des Registrierungsprozesses und sind nach Ablauf der dreißigtätigen Frist zu löschen, sofern keine Registrierung eines E-ID vorgenommen wurde.[295]

[292] ErläutRV 469 BlgNR 27. GP 6.
[293] Namen, Geburtsdatum, Pass- oder Personalausweisnummer und falls verfügbar eine E-Mail-Adresse.
[294] Weitere spezifische Regelungen zur Eingrenzung der Speicherdauer einzelner Merkmale finden sich bspw in § 4 Abs 6 E-GovG.
[295] ErläutIA 2227 BlgNR 26. GP 11.

4.5 Angaben über die Berücksichtigung der Betroffenenrechte

4.5.1 Gewährleistung der Transparenz und Informationspflichten

Über Art 12 ff DSGVO ist vorgeschrieben, dass der für die Datenverarbeitung *Verantwortliche* der betroffenen Person alle nach Maßgabe des Gesetzes erforderlichen Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt. Dabei geht es für die Betroffenen insb um transparente Information, Kommunikation und entsprechende Modalitäten zur Ausübung ihrer Rechte.

Dies wird zum einen in der Datenschutzinformation sichergestellt, auf welche im Zuge des Registrierungsprozesses mehrmals, erstmalig bei der Registrierung, verwiesen wird. Die Datenschutzinformation kann auch danach jederzeit entweder auf der Startseite der App, unter der Rubrik „Über Digitales Amt“ > „Datenschutz“ oder im Webaufritt des *Verantwortlichen* abgerufen werden.[296]

Zudem wird den Benutzer*innen vor jedem Anmeldevorgang ein Link zur anwendungsspezifischen Datenschutzerklärung jenes Service Providers, bei welchem die Anmeldung erfolgen soll, angezeigt. Besonders relevante Fragen im Zusammenhang mit dem ID Austria System wurden zudem über eine eigene Seite als „Frequently Asked Questions“ (FAQs) aufbereitet.[297]

4.5.2 Recht auf Auskunft und Datenübertragbarkeit

Die Betroffene haben gem Art 15 DSGVO das Recht, vom *Verantwortlichen* jederzeit auf Antrag eine Auskunft über die von diesem verarbeiteten, sie betreffenden personenbezogenen Daten zu erhalten. Zur Ausübung des Auskunftsrechts können Betroffene einen Antrag auf Auskunft beim *Verantwortlichen* einbringen. Die diesbezüglichen Kontaktdaten sind in der Datenschutzinformation angegeben.[298]

Weiters haben Betroffene nach Maßgabe des Art 20 DSGVO das Recht auf Datenübertragbarkeit, wobei die betreffenden Daten vom *Verantwortlichen* in einem strukturierten, gängigen, maschinenlesbaren Format zu übermitteln sind. In der Datenschutzinformation wird auf diesen Anspruch hingewiesen und die notwendigen Kontaktmöglichkeiten angegeben.[299]

4.5.3 Recht auf Berichtigung und Löschung

Gem Art 16 DSGVO haben Betroffene das Recht, vom *Verantwortlichen* die unverzügliche Berichtigung der sie betreffenden personenbezogenen Daten zu verlangen, sofern diese unrichtig sein sollten. Dies beinhaltet auch den Anspruch, eine Vervollständigung unvollständiger personenbezogener Daten

[296] Zum Zeitpunkt der Erstellung des Berichts unter https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html sowie im angemeldeten Bereich https://secure.oesterreich.gv.at/#/settings/gdpr (jeweils abgerufen am 22.04.2022).
[297] Siehe hierzu https://www.oesterreich.gv.at/themen/dokumente_und_recht/id-austria/haeufige-fragen/sicherheit-und-datenschutz.html (abgerufen am 22.04.2022).
[298] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022).
[299] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022).

mittels einer ergänzenden Erklärung zu verlangen. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation die erforderlichen Kontaktmöglichkeiten angegeben.[300]

Betroffene haben das Recht, unter den in Art 17 DSGVO beschriebenen Voraussetzungen vom *Verantwortlichen* die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Voraussetzungen sehen insbesondere ein Löschungsrecht vor, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, sowie in Fällen der unrechtmäßigen Verarbeitung; auch wenn Betroffene ihre Einwilligung[301] widerrufen und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt, besteht ein Recht auf Löschung. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation die erforderlichen Kontaktmöglichkeiten angegeben.[302]

Die Daten werden unverzüglich gelöscht, wenn der *Verantwortliche* nicht aufgrund von gesetzlichen Aufbewahrungspflichten dazu angehalten ist, die Daten aufzubewahren. Zu den einzelnen Fristen siehe Kapitel zur Speicherbegrenzung.

In den Materialien zum E-GovG wird zudem klargestellt, dass durch ein Löschungsersuchen gemäß Art 17 DSGVO weiterhin bewirkt werden kann, dass Daten, die im Zuge des Pilotbetriebs erhoben wurden, gelöscht werden.[303]

4.5.4 Recht auf Einschränkung und Recht auf Widerspruch

Das Recht auf Einschränkung der Verarbeitung und das Recht auf Widerspruch werden nach Maßgabe des Art 23 DSGVO iVm § 4b E-GovG eingeschränkt. Zur Einschränkung führen die Gesetzesmaterialien[304] wie folgt aus:

„Gemäß Art. 21 Abs. 1 DSGVO hat der Betroffene das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus hat der Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen.

Ein solches, dem Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung kann jedoch gemäß Art. 23 DSGVO zur Sicherstellung einer der in Abs. 1 lit. a bis j genannten Zwecke durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung wird in § 4b Abs. 2 für sämtliche zum Zwecke der Registrierung eines E-ID verarbeiteten Daten Gebrauch gemacht.

Die Registrierung des E-ID erfolgt stets unter Verarbeitung personenbezogener Daten in der zentralen Evidenz, die Registrierungsdaten sind dem qualifizierten VDA zur Ausstellung eines qualifizierten Zertifikats zu übermitteln. E-ID-Inhaber haben das Recht, zu jedem Zeitpunkt eine vorübergehende

[300] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022).
[301] In diesem Fall nur bei Informationsaussendungen für Auslandsösterreicher*innen.
[302] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022).
[303] ErläutRV 469 BlgNR 27. GP 9.
[304] ErläutRV 469 BlgNR 27. GP 4.

Aussetzung sowie einen Widerruf des E-ID bei der Behörde zu verlangen. § 4a Abs. 5 verpflichtet die Behörden zudem zur Aussetzung oder zum Widerruf eines E-ID, insbesondere, wenn sie Kenntnis vom Tod des E-ID-Inhabers oder einer drohenden Missbrauchsgefahr erlangen sowie für den Fall, dass Zweifel an der Identität des Betroffenen aufkommen. Eine Erfüllung dieser Aufgaben ist unmöglich, wenn die Daten aufgrund eines Widerspruchs des Betroffenen nicht verarbeitet werden dürfen. Den Behörden würde im Falle eines Widerspruchs jede Handlungsmöglichkeit entzogen, die missbräuchliche Verwendung – insbesondere auch die Verwendung eines E-ID mit einer zweifelhaften Identität – zu unterbinden.

Auch sonst ist es zu Beweiszwecken und zur Vermeidung allfälliger Amtshaftungsansprüche unumgänglich, dass das Bestehen eines gültigen E-ID und damit die Möglichkeit der Verwendung im Rechtsverkehr bzw. der Zeitpunkt einer Aussetzung oder eines Widerrufs von den Behörden nachvollzogen werden kann.

Die Ausübung dieser Rechte hätte zudem einen beträchtlichen Verwaltungsaufwand zur Folge, da einerseits die in § 4a Abs. 1 vorgesehene amtswegige Registrierung des E-ID rasch zu einer hohen Anzahl an E-ID-Inhabern führen wird und andererseits durch den Ausschluss des Widerspruchsrechts und des Rechts auf Einschränkung der Verarbeitung in § 22b Abs. 6 Passgesetz 1992 innerhalb eines Registers unterschiedliche datenschutzrechtliche Rahmenbedingungen geschaffen würden.

Die Gewährleistung einer geordneten Vollziehung des E-Government-Gesetzes durch die Registrierungsbehörden gemäß § 4a stellt aus den zuvor genannten Gründen ein wichtiges Ziel des allgemeinen öffentlichen Interesses dar (Art. 23 Abs. 1 lit. e DSGVO). Der Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO ist aus den zuvor genannten Gründen zwingend erforderlich. Die in § 4a Abs. 1 vorgesehene Möglichkeit eines „Opt-Outs“ bleibt unberührt.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an behördliche Register oder Dateisysteme, ausschließlich rechtmäßig verarbeitete personenbezogene Daten zu enthalten, umgehend zu löschen und soll es nicht möglich sein, dass der Betroffene lediglich die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. b und lit. c DSGVO verlangt.

Den für den Ausschluss des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung einschlägigen Vorgaben des Art. 23 Abs. 2 DSGVO wird entsprechend Rechnung getragen. So ergeben sich aus den gesetzlichen Vorgaben zur Verarbeitung von personenbezogenen Daten nach diesem Bundesgesetz für den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO insbesondere sowohl der Umfang der vorgenommenen Beschränkung und die Kategorien der betreffenden personenbezogenen Daten als auch die für deren Verarbeitung Verantwortlichen und Zwecke sowie die jeweiligen Speicherfristen. Der Ausschluss des Rechts auf Widerspruch gegen die Verarbeitung von personenbezogenen Daten bezieht sich überdies selbstverständlich ausschließlich auf jene Daten, die in Übereinstimmung mit den gesetzlichen und unionsrechtlichen Vorgaben in rechtskonformer Weise verarbeitet werden. Den Betroffenen bleibt es zudem auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen oder unrechtmäßig verarbeiteten personenbezogenen Daten oder

personenbezogenen Daten, deren Verarbeitung für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig ist, von ihrem Recht auf Berichtigung und Löschung gemäß den Art. 16 bis 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher auch kein Rechtsschutzdefizit.

Als grundrechtsschützende Maßnahme und in Umsetzung des Art. 23 Abs. 2 lit. h DSGVO ist im letzten Satz vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind. Ausdrücklich steht es den Registrierungsbehörden dabei frei, diese Information nicht an jeden einzelnen Betroffenen individuell, sondern an „die Betroffenen" in deren Gesamtheit zu richten. Die Information kann daher auch in allgemeiner Weise erteilt werden (z. B. auf einer Homepage).

Die Ausführungen lassen erkennen, dass das in der DSGVO vorgesehene Recht auf Widerspruch sowie das Recht auf Einschränkung der Verarbeitung in einem Spannungsverhältnis zur gesetzlich angeordneten Datenverarbeitung stehen. Die Bestimmung stellt demzufolge eine ausgewogene Abwägung zwischen den administrativen Interessen sowie dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar und soll die geordnete Vollziehung durch die Registrierungsbehörden sowie die Funktionalität und die ordnungsgemäße Führung der zentralen Evidenz gewährleisten."

4.5.5 Recht auf Beschwerde

Darüber hinaus haben Betroffene, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt, gem Art 77 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde. Auch hierfür sind die notwendigen Kontaktdaten in der Datenschutzinformation zu finden.[305]

[305] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022). Die zuständige Aufsichtsbehörde ist die Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, A-1030 Wien Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at, Web: https://www.dsb.gv.at.

4.6 Datenschutzrechtliche Anforderungen an die Protokollierung

Bevor im Rahmen dieses DSFA-Berichts auf die konkrete Ausgestaltung der Protokollierung mit Fokus auf die Risikoanalyse eingegangen wird, sollen im Folgenden die datenschutzrechtlichen Rahmenbedingungen[306] **überblicksartig** dargestellt werden.

Vorauszuschicken ist bereits an dieser Stelle, dass der Begriff der „Protokollierung" in der DSGVO nicht ausdrücklich genannt wird. Die Vornahme einer Protokollierung von Verarbeitungsvorgängen kann sich jedoch einerseits insb aus der Rechenschafts- und Nachweispflicht des *Verantwortlichen* (siehe Art 5 Abs 2 und Art 24 Abs 1 DSGVO),[307] andererseits auch aus Anforderungen an die Datensicherheit (Art 32 DSGVO)[308] ergeben. Daneben existiert in Bezug auf Einwilligungen gem Art 7 Abs 1 DSGVO eine spezifische Nachweispflicht, wonach der *Verantwortliche* die erfolgte Einwilligung der jeweils betroffenen Person nachweisen können muss, was ebenfalls im Ergebnis zu einer Protokollierung führen wird.[309]

Unmittelbar wird eine Protokollierung von Verarbeitungsvorgängen in § 50 DSG normiert, wobei diese Bestimmung in Umsetzung der JI-RL (EU) 2016/680 ergangen ist und daher nur einen (im vorliegenden Kontext nicht erfüllten) eingeschränkten Anwendungsbereich hat.[310]

Bei Protokolldaten handelt es sich nach der Entscheidungspraxis der Datenschutzbehörde idR um personenbezogene Daten.[311] Generell gilt es zu beachten, dass es durch die Vornahme einer Protokollierung auch zu einer eigenen Verarbeitung von Daten kommt,[312] welche (bei Vorliegen personenbezogener Daten) einer Rechtsgrundlage gem Art 6[313] bzw (bei Vorliegen sensibler Daten) Art 9 (jeweils iVm Art 5 bzw Art 32 DSGVO) bzw einer entsprechenden Norm im Unionsrecht oder dem nationalen Recht bedarf.

---

[306] Betrachtet werden im Folgenden vorrangig die Vorgaben aus der DSGVO und dem DSG.

[307] Siehe die Stellungnahme der Datenschutzbehörde zu dem Ministerialentwurf betreffend Bundesgesetz, mit dem das Bundesstatistikgesetz 2000 und das Forschungsorganisationsgesetz geändert werden, 38/SN-135/ME 27. GP 8: Protokollierung sei [Anm: im vorliegenden Kontext] jedenfalls als Schutzfunktion zu werten, die es dem Verantwortlichem ermöglicht, seiner Rechenschaftspflicht nachzukommen; SDM, Baustein 43 „Protokollieren" (Version 1.0a) 1; siehe https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (abgerufen am 22.04.2022); im Ergebnis einschränkend *Veil*, Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO?, ZD 2018, 9 (11, 13, 16).

[308] ENISA, Handbook on Security of Personal Data Processing (2017) 58 uam (unter Hinweis auf ISO/IEC 27001:2013); siehe jüngst die Empfehlungen zur Protokollierung – unter ausdrücklicher Bezugnahme auf Art 5 u 32 DSGVO – der franz Datenschutzbehörde CNIL, Délibération no 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation 1; siehe auch das dt. Standarddatenschutzmodell (SDM), Baustein 43 „Protokollieren" (Version 1.0a) 1; unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (abgerufen am 22. 04. 2022); siehe zur Protokollierung als explizite Datensicherheitsmaßnahme § 14 Abs 1 Z 7 DSG 2000 (nicht mehr in Kraft).

[309] Ausf dazu *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO Rz 12 ff (Stand 7.5.2020, rdb.at).

[310] § 50 DSG ist somit nur auf die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs anwendbar; auf die Protokollierung gem § 13 Abs 2 u 3 DSG wird an dieser Stelle mangels Relevanz nicht eingegangen.

[311] Vgl. dazu bspw. DSB, Empfehlung vom 31. 01.2017, DSB-D213.471/0005-DSB/2016.

[312] *Hötzendorfer/Kastelitz* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Datenschutzgesetz (2018) § 50 Anm 1.

[313] In Frage kommt hier inbs Art 6 Abs 1 lit c (Erfüllung einer rechtlichen Verpflichtung; Archivierungspflicht), siehe *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO Rz 13 mwN (Stand 7.5.2020, rdb.at) oder Art 6 Abs 1 lit f (IT-Sicherheit) *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 54 (Stand 7.5.2020, rdb.at), wobei lit f gem Art 6 Art 1 letzter Satz DSGVO nicht für die von Behörden in Erfüllung ihrer [hoheitlichen] Aufgaben vorgenommene Verarbeitung gilt; jüngst auch Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung. Orientierungshilfe (2021) Rz 121.

Soweit die Aufzeichnung von Verarbeitungsvorgängen im Einzelfall nicht ausdrücklich gesetzlich angeordnet ist, wird sich die Zulässigkeit (bzw Unzulässigkeit) sowie in der Folge der Umfang der Durchführung einer Protokollierung aus einer **Gesamtbetrachtung** der Datenverarbeitung unter besonderer Beachtung des Grundsatzes der **Verhältnismäßigkeit** ergeben.[314] Dieser spiegelt sich (neben § 1 Abs 2 letzter Satz DSG)[315] auch in den datenschutzrechtlichen Prinzipien der Datenminimierung (Art 5 Abs 1 lit c DSGVO), der Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO) und der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO)[316] wider. Der Grundsatz der Verhältnismäßigkeit erfordert, dass eine Verarbeitung personenbezogener Daten

- einem legitimen Zweck dient (siehe dazu unter 4.6.3),
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen, und
- angemessen, dh verhältnismäßig im engeren Sinne, ist.[317]

Der Grundsatz der Erforderlichkeit besagt, dass eine Verarbeitung personenbezogener Daten nur so weit zulässig ist, als dies für die Erreichung des damit verfolgten Zwecks notwendig ist,[318] es also kein milderes, gleich effektives Mittel gibt. Im Rahmen von Protokollierungsvorgängen wird die Erforderlichkeit einer Protokollierung (und deren Umfang) insb anhand des konkreten **Verarbeitungskontextes**, des **Schutzbedarfs** und der **Risikobewertung** zu beurteilen sein.

In diesem Zusammenhang ist auch Art 5 Abs 1 lit c DSGVO relevant, der die Verarbeitung personenbezogener Daten von der Einhaltung des Grundsatzes der **Datenminimierung** abhängig macht. Laut EuGH geht aus dem Wortlaut dieser Bestimmung hervor, dass mit diesem Prinzip kein allgemeines und absolutes Verbot (der Datenverarbeitung) eingeführt werden soll.[319] Daraus ergibt sich in einer **Gesamtbetrachtung** bei der Speicherung von Protokolldaten also kein Verbot, sondern eine Prüfung auf die Einhaltung des Verhältnismäßigkeitsgrundsatzes im Einzelfall und insbesondere der konkret erforderlichen Datenfelder für die Zweckerreichung der Protokollierung.

Bereits auf Basis des Vorstehenden ist somit die Zulässigkeit einer generellen Vorratsdatenspeicherung durch eine (zeitlich und inhaltlich) uferlose Protokollierung ausgeschlossen. Insbesondere bei häufig benutzten Systemen, wie zB bei einem umfassenden Identitätssystem, ist zu beachten, dass die Zusammenführung und Auswertung von in Protokolldateien erfassten Nutzer*innenaktivitäten ein detailliertes Personenprofil ergeben[320] bzw eine weitgehende Überwachung von Nutzer*innen

---

[314] Vgl bereits zum DSG 2000 *Jahnel*, Handbuch Datenschutzrecht [2010] 304 Rz 5/24; siehe auch *Hötzendorfer/Kastelitz* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Datenschutzgesetz (2018) § 50 Anm 1.

[315] Dieser lautet: „Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden".

[316] *Martini* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 5 Rz 37 (Eingabekontrolle durch Protokollauswertung).

[317] Siehe zB *Bock/Kühne/Mühlhoff/Ost/Rehak/Pohle*, Datenschutz-Folgenabschätzung für die Corona-App, Version 1.6 vom 29. 4. 2020, 61.

[318] Siehe *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 19 mwN (Stand 7.5.2020, rdb.at). Gem EuGH 16. 12. 2008, C-524/06 handelt es sich beim Begriff der Erforderlichkeit um einen autonomen Begriff des Unionsrechts, der so auszulegen ist, dass er in vollem Umfang dem Ziel der Richtlinie [Anm: DSRL 95/46/EG als „Vorgängerin" der DSGVO) entspricht.

[319] EuGH 22. 6.2021, C-439/19 Rz 104.

[320] Siehe zu einigen Gefahren des Profiling (allerdings im Zusammenhang mit Webtracking) *Gräfe*, Webtracking und Microtargeting als Gefahr für Demokratie und Medien, PinG 2019, 5 ff; zu Gefährdungspotentialen durch Erhebung und Verknüpfung von Profildaten im digitalisierten Alltag siehe auch *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht[7], Kap 9 Rz 4 f (Stand: 02.11.2021).

ermöglichen können und daher angemessene technische und organisatorische Maßnahmen zu treffen sind, die diesem Risiko effektiv entgegenwirken.

4.6.1 Was versteht man unter „Protokollierung“?

Bei der Protokollierung in (wie hier) automatisierten Verarbeitungssystemen werden alle oder ausgewählte Aktivitäten (bzw im datenschutzrechtlichen Sinne Verarbeitungsvorgänge iSd Art 4 Z 2 DSGVO, wie zB Speicherung, Veränderung, Abfragen, Abgleichen, Löschen)[321] zusammen mit weiteren Metadaten, wie Datum und Zeit des jeweiligen Vorganges (Timestamp), aufgezeichnet. Ergebnis der Speicherung dieser Protokolldaten sind sogenannte „Protokolle“ – auch „Logfiles“ oder „Protokolldateien“ genannt. Laut dem deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) kann grundsätzlich zwischen zwei Protokollierungsebenen unterschieden werden:[322]

- Protokollierung technischer Systemereignisse auf **Ebene der IT-Infrastruktur (Infrastrukturebene)** zum Zweck der Überwachung der IT-Sicherheit bzw der Datensicherheit[323] (zB Erkennung unbefugter Aktivitäten) sowie der Sicherstellung der ordnungsgemäßen Funktion bzw der Verifizierung und Behebung von Systemfehlern[324]
- Datenschutzrechtlich normierte Protokollierung auf **fachlicher Ebene (Anwendungsebene)**[325], die insbesondere dem Ziel dient, eine effiziente Nachprüfbarkeit einzelner Verarbeitungsvorgänge zu ermöglichen, worunter auch die Eigenkontrolle fällt.[326] Zu den protokollierten Vorgängen zählen – abhängig von der konkreten Ausgestaltung – insbesondere Aktivitäten der Nutzer*innen (User) der Anwendungen, wozu sowohl Administrator*innen als auch Endnutzer*innen zählen.

Da es sich beim Vorstehenden aufgrund der Komplexität moderner IT-Landschaften nur um eine grobe schematische Einordnung handeln kann, sind weitere Unterteilungen und Unterscheidungen möglich; so kann die Protokollierung zB auf Anwendungsebene nach Nutzer*innengruppen aufgespalten sein.

---

[321] Tlw auch als „Transaktionsdaten“ bezeichnet.

[322] Vgl BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 1, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_Protokollierung.pdf?__blob=publicationFile&v=2 (abgerufen am 22.04.2022).

[323] Siehe zB *Schallbruch*, Das IT-Sicherheitsgesetz 2.0 – Befugnisse des BSI und Schutz der Bundesverwaltung, CR 2021, 516 (519): „Im Lichte jüngster Cyberangriffe auf Einrichtungen des Bundes […] kommt der Auswertung von Protokolldaten eine besondere Bedeutung zu, um Zeitpunkt des Eindringens, Urheber und Methodik des Angriffs sowie den Umfang der betroffenen Systeme zu ermitteln.“

[324] Auch der Europäische Datenschutzbeauftragte geht von einer Protokollerstellung zur Rekonstruktion von Ereignissen im IT-System aus, EDPS, Leitlinien zum Schutz personenbezogener Daten für die Bereiche IT-Governance und IT-Management der EU-Institutionen (2018) Rz 107, abrufbar unter https://edps.europa.eu/sites/default/files/publication/it_governance_management_de.pdf (abgerufen am 22.04.2022).

[325] In Deutschland auch „Fachanwendungsebene“ genannt, siehe BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 1; SDM, Baustein 43 „Protokollieren“ (Version 1.0a) 4: „Fachapplikation“.

[326] Die DSB hat anlässlich ihrer Schwerpunktprüfungen von Krankenanstalten ua die regelmäßige (interne) Nachkontrolle der Zugriffsprotokolle auf Patientendaten verlangt, siehe zB DSB 31. 1. 2017, DSB-D213.471/0005-DSB/2016 und den Überblick bei *Haidinger*, Datenschutz bei Patientendaten, Dako 2016/54.

4.6.2 Inhalt von Protokolldaten

Da es kaum einheitliche Datenverarbeitungen gibt und sich diese samt der dabei jeweils anfallenden Daten unter anderem hinsichtlich **Verarbeitungskontext**, **Schutzbedarf** und **Risikobewertung** idR unterscheiden werden, sind die Inhalte einer stattfindenden Protokollierung abhängig von der **konkreten Anwendung** und dem verfolgten **Protokollierungszweck**, wobei an dieser Stelle auch auf die obigen Ausführungen zum Grundsatz der Verhältnismäßigkeit zu verweisen ist. So wird im Österr Informationssicherheitshandbuch dazu ausgeführt, dass „Art und Umfang von Protokollierungen von den speziellen Anforderungen des IT-Systems und der darauf befindlichen Applikationen und Daten ab[hängen] und im Einzelfall sorgfältig festzulegen [sind].“[327]

Beispielhaft muss bei Vorliegen des Protokollierungszwecks „Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ aus **datenschutzrechtlicher** Sicht anhand der Logdateien verifiziert werden können, **wer wann welche** personenbezogenen Daten **wie** verarbeitet hat. So wird im deutschen Standarddatenschutzmodell (SDM) gefordert, dass zur vollständigen Prüfung zumindest die folgenden Protokolldaten notwendig sind:[328]

a) Zeitkomponente („Wann?“)
b) Instanz, die eine Aktivität auslöst („Wer?“)
c) Aktivität bzw Ereignis, das durch die Instanz ausgelöst wurde („Was?“)
d) Speicherinstanz (Quelle und Ziel), die diese Protokolldaten speichert („Protokollierung durch wen?“)

Andere Anforderungen an die Inhalte der Protokolldatei können sich bei der Protokollierung zum Zweck der Überwachung der IT-Sicherheit und der Sicherstellung der ordnungsgemäßen Funktion auf der Infrastrukturebene ergeben.

4.6.3 Wozu wird protokolliert?

Als üblicher Zweck der Protokollierung (aus Sicht des Datenschutzrechts und insbesondere der Datensicherheit) ist vor allem die Nachprüfbarkeit der datenschutzrechtlich relevanten Vorgänge anzuführen. Diese Nachprüfbarkeit einzelner Verarbeitungsvorgänge ist dabei Grundvoraussetzung für die Erbringung eines Nachweises der Einhaltung der rechtlichen Datenschutzanforderungen durch den *Verantwortlichen* (Rechenschaftspflicht gem Art 5 Abs 2 DSGVO).[329] Die Kontrollierbarkeit der Ordnungsmäßigkeit der Datenverarbeitung durch Protokollierung ist gleichzeitig auch eine Maßnahme zur Sicherstellung von Informations- und Datensicherheit.[330]

Weitere Zwecke können zB die Eigenüberwachung, die Gewährleistung von Integrität und Sicherheit personenbezogener Daten (Art 32 DSGVO) sowie die Verwendung in gerichtlichen Strafverfahren und bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sein.

[327] Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[328] Vgl SDM, Baustein 43 „Protokollieren“ (Version 1.0a) 2 f.
[329] Vgl SDM, Baustein 43 „Protokollieren“ (Version 1.0a) 1; https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (abgerufen am 22.04.2022).
[330] Siehe Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.

Der Zweck der Protokollierung besteht aber auch darin, eine Verarbeitung personenbezogener Daten transparent zu gestalten und betroffenen Personen über die Verarbeitung ihrer Daten auf Nachfrage eine Auskunft erteilen zu können.[331]

4.6.4 Auswertung von Protokollen

Soweit keine Rechtsnorm die Auswertung von Protokolldaten ausdrücklich regelt, ergeben sich aus dem allgemeinen datenschutzrechtlichen Grundsatz der Zweckbindung enge Grenzen für deren Auswertung; so wird sich idR aus den initial definierten Zwecken für das Erfassen von Protokolldaten auch die zulässige Zielsetzung der Auswertung ergeben.

Protokolldaten dürfen somit nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck unvereinbar sind. Beispielhaft dürfen gem § 50 Abs 4 DSG „[…] Protokolle ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung einschließlich der Eigenüberwachung, der Gewährleistung von Integrität und Sicherheit der personenbezogenen Daten sowie in gerichtlichen Strafverfahren verwendet werden".

Mit Bezug auf § 18 Abs 1 letzter Satz E-GovG kann aus dem Gesetzeswortlaut und den Materialien[332] abgeleitet werden, dass es dem *Verantwortlichen* und dem *Auftragsverarbeiter* nicht verwehrt ist, den Grundsätzen für die Verarbeitung personenbezogener Daten nachzukommen, worunter zB im Rahmen der Überprüfung der Rechtmäßigkeit der Datenverarbeitung auch die (interne) Auswertung von Protokolldaten fallen wird. Es ist jedoch darauf zu achten, dass dabei nur die im Einzelfall relevanten (personenbezogenen) Daten ausgewertet werden dürfen.

Unterstützend kann für diese Ansicht auch die Durchführungsverordnung (EU) 2015/1502 herangezogen werden, die Folgendes in ihrem Anhang unter Pkt 2.4.4. (Aufbewahrungspflichten) vorsieht: „Die Aufzeichnung und Aufbewahrung einschlägiger Informationen erfolgt mit einem effektiven Aufzeichnungsverwaltungssystem unter Beachtung geltender Vorschriften und bewährter Verfahren auf dem Gebiet des Datenschutzes und der Datenspeicherung. 2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet."[333]

Hinzuweisen ist an dieser Stelle, dass für die Verarbeitung (worunter auch die Auswertung zählt) von Protokolldaten selbst angemessene technische und organisatorische Maßnahmen gem Art 32 DSGVO zu treffen sind, wie zB Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (Wer hat Zugriffsrechte worauf?; Vier-Augen-Prinzip bei der Auswertung; kein „Super-User", der alleine alle

[331] Vgl *bvitg/gmds/IHE Deutschland*, Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen (2020) 12, abrufbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php (abgerufen am 22.04.2022).
[332] ErläutRV 469 BlgNR 27. GP 7.
[333] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, ABl L 235, 7 (18) vom 9. 9. 2015 (Hervorhebung nicht im Original).

vorhandenen Dateien zusammenführen kann) sowie technische Maßnahmen zur Gewährleistung der Revisionssicherheit der Protokolldaten (Manipulationsschutz).[334] Kurz gesprochen: Je höher das (potentielle) Risiko der Verarbeitung für die betroffenen Personen ist, desto umfangreicher muss der Schutz der Protokolldaten ausfallen.

4.6.5 Wie lange dürfen Protokolle aufbewahrt werden?

Konkrete Aufbewahrungsfristen für Protokolldaten finden sich weder in der DSGVO noch im geltenden DSG. Bis zum Ablauf des 24.5.2018 waren gem § 14 Abs 5 DSG 2000 Protokoll- und Dokumentationsdaten grds drei Jahre lang aufzubewahren, sofern gesetzlich nicht ausdrücklich anderes angeordnet war.

Mangels ausdrücklicher Anordnung der Speicherdauer durch eine Rechtsnorm (welche aus grundrechtlicher Sicht selbstverständlich in verhältnismäßiger Weise ausgestaltet sein muss) ergibt sich die Aufbewahrungsdauer aus dem Vorliegen der Erforderlichkeit für den jeweiligen Auswertungszweck. Wie lange dieses Kriterium der Erforderlichkeit vorliegt, ist häufig das Ergebnis einer Abwägung, in die neben dem Zweck auch Art und Inhalt der protokollierten Ereignisse und das Ergebnis einer Risikobewertung einfließen können.[335]

In diesem Sinne hat der Gesetzgeber in den Materialien zur Protokollierung gem § 50 DSG nachvollziehbar (und uE verallgemeinerungsfähig) erläutert, dass „[…] Protokolldaten – wie auch alle anderen personenbezogenen Daten – nur solange in personenbezogener Form aufbewahrt werden [sollten], als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; danach sind die Protokolldaten zu löschen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen. Eine längere Aufbewahrungsdauer muss sich aus besonderen gesetzlichen Vorschriften ergeben".[336] Zumindest personenbezogene Teile von Protokolldaten sind daher nach Zweckerreichung zu löschen bzw zu anonymisieren,[337] sofern keine sonstigen gesetzlichen Fristen mehr bestehen.[338]

Interessant sind die (allerdings im Rahmen eines Art 36 DSGVO-Verfahrens im Bereich einer deutschen Rundfunkanstalt ergangenen) Ausführungen zur Speicherdauer von Logdaten zur Feststellung bzw Abwehr von Cyberattacken.[339] Obwohl deutsche Rundfunkanstalten (jedenfalls zum Zeitpunkt der Entscheidungsfindung) nicht als Betreibende einer kritischen Infrastruktur zu qualifizieren waren, verwies der Rundfunkdatenschutzbeauftragte auf die Empfehlung des BSI an Betreibende kritischer Infrastrukturen iSd deutschen BSI-Gesetzes, welche die Speicherung von Logdaten, jedenfalls für

[334] Instruktiv dazu BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 5.
[335] Siehe dazu Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[336] ErläutRV 1664 BlgNR 25. GP 23.
[337] Beispielsweise können Protokolldaten mit Personenbezug anonymisiert werden, sofern nur noch Metadaten (die keinen Personenbezug aufweisen, Achtung ist daher geboten bei Vorhandensein von IP-Adressen etc) des protokollierten Ereignisses relevant sind, vgl Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[338] Vgl ErläutRV 1664 BlgNR 25. GP 23.
[339] Siehe Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für das Jahr 2019 Rz 160 ff, https://www.zaftda.de/tb-oe-r-rundfunkanstalten/783-zdf-tb-dsb-2019/file (abgerufen am 22.04.2022).

Proxy- und Firewall-Logs, für die Dauer von mindestens 90 Tagen vorsieht.[340] Bei zu erwartenden Beschwerden an die Datenschutzbehörde wäre auch die Heranziehung der Fristen in § 24 Abs 4 DSG denkbar. Für die kommende eIDAS 2-VO schlägt ein renommierter Experte eine Aufbewahrungsdauer zwischen zwei Jahren und einem Monat vor, welche aufgrund einer durchgeführten DSFA festzulegen sei.[341]

Das Ergebnis hinsichtlich der Speicherdauer von Protokolldaten muss uE – nicht zuletzt für die interne Umsetzung der Protokollierung und die (externe) Vorlage in einem etwaigen Verfahren vor der Datenschutzbehörde bzw vor Gericht – durch den *Verantwortlichen* niedergeschrieben, also dokumentiert werden. Hierfür ist die Erstellung eines sogenannten Protokollierungskonzepts empfehlenswert.[342]

4.6.6 Exkurs: Auskunftsrecht der betroffenen Personen

Teil der Betroffenenrechte ist das in Art 15 DSGVO normierte Recht auf Auskunft darüber, ob über die (anfragende) betroffene Person personenbezogene Daten verarbeitet werden. Da das Auskunftsrecht (bis auf Rechte und Freiheiten anderer Personen, siehe Art 15 Abs 4 leg cit; beachte auch § 4 Abs 5 und 6 DSG zur Gefährdung gesetzlich übertragener Aufgaben bzw von Geschäfts- oder Betriebsgeheimnissen) nicht weiter eingeschränkt wird, werden davon grds auch (personenbezogene) Protokolldaten erfasst sein, da der EuGH in seiner bisherigen Rsp dieses Betroffenenrecht tendenziell weit ausgelegt hat.[343] Dass jedoch noch Unklarheiten bei der Auslegung der DSGVO bestehen, die auch Art 15 betreffen, zeigt das rezente Vorabentscheidungsverfahren vor dem EuGH, worin auch das Auskunftsrecht über Protokolldaten thematisiert wird.[344]

Eine Umgehung des (verfassungsrechtlich in § 1 Abs 3 Z 1 DSG und Art 8 Abs 2 GRC festgeschriebenen) Auskunftsrechts durch fehlendes Anlegen von Protokollen, wo dieses gem Art 5 Abs 2 oder Art 32 DSGVO oder sonstige Rechtsgrundlagen erforderlich ist, ist wohl nicht rechtskonform. So hat die DSB auf Grundlage von Art 5 Abs 2 DSGVO entschieden, dass sich ein *Verantwortlicher* der Einhaltung seiner durch die DSGVO auferlegten Pflichten nicht dadurch entziehen kann, indem er ungeeignete technische und organisatorische Maßnahmen trifft, die es ihm ua verunmöglichen, den Anträgen von betroffenen Personen zu entsprechen.[345]

---

[340] BSI, Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen (2021) 12; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf?__blob=publicationFile&v=5 (abgerufen am 22.04.2022).

[341] *Olejnik*, Privacy analysis of European eID Regulation proposal (Pkt 13), https://blog.lukaszolejnik.com/privacy-analysis-of-european-eid-regulation-proposal/ (zuletzt abgerufen am 22. 04. 2022): „In Article 6a(7): ‚The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services.' It should also be defined that the collected information is deleted when not needed: after a time as defined in the DPIA documents prepared. Such a time period may be stipulated in the Regulation itself. It should not exceed two years, possibly even a month?"

[342] Siehe für die erforderlichen Inhalte instruktiv *bvitg/gmds/IHE Deutschland*, Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen (2020), abrufbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php (abgerufen am 22.04.2022).

[343] Siehe insb EuGH 20. 12. 2017, C-434/16 Rn 56 f (zur DSRL ergangen, aufgrund der ähnlichen Textierung in der DSGVO jedoch übernehmbar).

[344] Anhängig unter C-579/21.

[345] DSB 23. 7. 2019, DSB-D123.822/0005-DSB/2019.

Allerdings kann uE nach Vornahme einer dokumentierten Abwägung zwischen den hier aufeinanderprallenden Interessen, wie zB einerseits auf Auskunft, andererseits insb auf Hintanhaltung der (potentiellen) Generierung detaillierter Profildaten, der vorliegende Zielkonflikt durch Technikgestaltung und durch Setzen datenschutzfreundlicher Voreinstellungen gem Art 25 DSGVO im System weitgehend aufgelöst werden. Selbstverständlich ist die betroffene Person darüber in Kenntnis zu setzen, so zB über eine sich daraus eventuell ergebende verkürzte Aufbewahrungsdauer ihrer personenbezogenen Daten.

4.6.7 Umsetzungsstrategie zur Protokollierung im Rahmen der ID Austria

Vorauszuschicken ist, dass es derzeit, soweit ersichtlich, an konkreten Best-Practice-Beispielen im Bereich von Identitätssystemen mangelt; insbesondere konnten keine veröffentlichten Protokollierungskonzepte aufgefunden werden, welche von einer (zuständigen) Datenschutzbehörde geprüft worden wären. Aufbauend auf den datenschutzrechtlichen Ausführungen zur Protokollierung wurden während der Durchführung der DSFA mehrere Vorschläge und Varianten hinsichtlich der konkreten Umsetzung der Protokollierung im ID Austria System diskutiert. Im Kern und ohne die obenstehenden Ausführungen hier im Detail zu wiederholen, sind **Art, Umfang und Dauer der Protokollierung** auf das zur Erfüllung des **Protokollierungszwecks erforderliche Maß** zu beschränken und entsprechende **technische und organisatorische Maßnahmen** zum Schutz von angelegten Protokolldaten zu treffen.

4.6.7.1 Umsetzung der Protokollierung

Zur serverseitigen Protokollierung kann wie folgt festgehalten werden:

Zweck(e): interne Nachkontrolle von Verarbeitungsvorgängen (insb durch internen *Datenschutzbeauftragten*); Transparenz der Verarbeitung personenbezogener Daten (Erfüllung der Rechte der betroffenen Personen).

Erfasste Datenkategorien:

- Transaktions-ID – Eindeutiger Identifikator der Transaktion
- Datum und Zeit der Transaktion (Timestamp)
- bPK ZP-MH der betroffenen Person, die die Transaktion ausführt
- Liste der im MDS enthaltenen und vom E-ID System übermittelten Attribute (ohne die konkreten Attributwerte)
- Liste der im Zuge der Transaktion vom E-ID System übermittelten zusätzlichen, dh über das MDS hinausgehenden, Attribute (ohne die konkreten Attributwerte)
- In die Transaktion involvierter Service Provider
- Information zur Erbringung der notwendigen Einwilligung zur Datenverarbeitung entsprechend einer der beiden folgenden Varianten:

- Explizite (transaktionsbasierte) Einwilligung im Zuge der Transaktion: Einwilligung muss für Transaktion protokolliert werden (Web, App)
- Implizite (dauerhafte) Einwilligung aufgrund vorheriger Einwilligung, die bis auf Widerruf oder bis Änderung des Attribut-Sets, maximal aber für ein Jahr, gültig bleibt: Datum dieser (nach wie vor gültigen) Einwilligung muss für jede Transaktion protokolliert werden (nur App)

Zusätzlich sind die Attribut-Sets revisionssicher im SPRS abgelegt (das Attribut-Set zu SP X hat zum Zeitpunkt Y wie folgt ausgesehen: Attribut A, Attribut B, Attribut C). Hinsichtlich der konkreten Daten muss die SZRB die Benutzer*innen auf die Empfänger*innen/Service Provider verweisen. Diese Festlegung ist ein Kompromiss zwischen der Gewährleistung von Betroffenenrechten (inklusive dem Datenzugang) und der Datenminimierung.

Speicherdauer: ein (1) Jahr. Begründung: Die relative Beschwerdefrist beträgt ein Jahr ab Kenntnis des beschwerenden Ereignisses nach § 24 Abs 4 DSG.[346] Auch interne Datenschutzkontrollen werden innerhalb eines Jahres stattfinden.

Geeignete technische und organisatorische Maßnahmen: Um die mit der Protokollierung verbundenen Risiken zu mitigieren (und zu erwartende Kritik „abzumildern“) sind (möglichst umfassende) TOM zu treffen; siehe weiter unten Pkt 4.7.7.3.

Mögliche (datenschutzrechtliche) Rechtsgrundlage(n) für die Protokollierung: In Frage kommen insbesondere Art 6 Abs 1 lit c, e bzw f[347] DSGVO (wobei hier davon ausgegangen wird, dass keine „sensiblen“ Daten gem Art 9 Abs 1 DSGVO verarbeitet werden).[348]

Abhängig von der Wahl der Rechtsgrundlage besteht ein **Recht auf Widerspruch**. Art 21 Abs 1 DSGVO lautet: „Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben **e oder f** erfolgt, Widerspruch einzulegen; […] Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.“

Eine Protokollierung erfolgt idR zur Erfüllung mehrerer berechtigter Zwecke (zT wohl auch im Interesse der betroffenen Person selbst), ua zur Auskunftserteilung und der Kontrolle der Verarbeitung, was oftmals (als **zwingende schutzwürdige** Gründe) gegen eine daraus folgende Löschung sprechen wird.

---

[346] „Der Anspruch auf Behandlung einer Beschwerde erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt. Verspätete Beschwerden sind zurückzuweisen.“ Hinzuweisen ist aus Sicht des RI in diesem Zsh, dass dies uE eine vertretbare Rechtsansicht darstellt, jedoch bislang belastbare Judikatur dazu fehlt.

[347] Hinweis: Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

[348] Siehe zu Art 6 Abs 1 lit c bzw f DSGVO die Ansicht des BSI, Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen (2021) 8, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf?__blob=publicationFile&v=5 (abgerufen am 22.04.2022).

Ob sich eine Datenverarbeitung „Protokollierung“ auf Art 6 Abs 1 lit c DSGVO („die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt“) stützen kann, hängt vom Vorliegen einer solchen Rechtspflicht ab. Hier könnten auch unmittelbar anwendbare unionsrechtliche Normen (Rechenschaftspflicht gem Art 5 Abs 2, Nachweispflicht aus Art 7 Abs 1 und Pflicht zur Gewährleistung von Datensicherheit gem Art 32 DSGVO) sowie die Durchführungsverordnung (EU) 2015/1502 (insb Pkt 2.4.4. Aufbewahrungspflichten) herangezogen werden (wobei es dazu an einschlägiger Judikatur fehlt). So leitet der Bayerische Landesbeauftragte für den Datenschutz aus Art 7 Abs 1 DSGVO eine Rechtspflicht ab: „Die vom Verantwortlichen zu erfüllende gesetzliche Verpflichtung ist hier die Nachweispflicht aus Art. 7 Abs. 1 DSGVO.“ [349] Da es im Rahmen der Protokollierung auch zur Aufzeichnung der Einwilligungserteilung kommt, kann jedenfalls dieser Teil auf Art 6 Abs 1 lit c iVm Art 7 Abs 1 DSGVO gestützt werden.

Bei der Protokollierung erfolgt keine Unterscheidung zwischen öffentlich-rechtlichen und privaten Service Providern.

4.6.7.2 Zur Geltungs- und Speicherdauer von Einwilligungen

Da es im Rahmen des ID Austria Systems auch zur Verarbeitung auf Grundlage von Einwilligungen kommt, ist auf die Geltungs- und Speicherdauer der eingeholten Einwilligungserklärungen einzugehen. Zu unterscheiden ist zunächst zwischen der Geltungsdauer einer Einwilligung zur Rechtfertigung der Einwilligung und der Speicherdauer (Aufbewahrung) des Nachweises der erteilten Einwilligung:

Dauer der Gültigkeit der Einwilligung: Aus den EDSA-Leitlinien lässt sich hierzu anführen, dass die DS-GVO „keine spezifische Frist [enthält], wie lange eine Einwilligung gilt. Wie lange die Einwilligung gültig ist, hängt vom Kontext, dem Umfang der ursprünglichen Einwilligung und den Erwartungen der betroffenen Partei ab. Wenn sich die Verarbeitungsvorgänge beträchtlich ändern oder weiterentwickeln, ist die ursprüngliche Einwilligung nicht länger gültig. Dann muss eine neue Einwilligung eingeholt werden.“ [350]

Speicherdauer zum Nachweis der erteilten Einwilligung: Aus Art 7 Abs 1 DSGVO ergibt sich eine spezifische Nachweispflicht des *Verantwortlichen* (und daher idR eine Aufzeichnungspflicht). Diese Norm lautet: „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.“

Der Europäische Datenschutzausschuss (EDSA) postuliert jedenfalls für die Dauer der jeweiligen Datenverarbeitungstätigkeit die Pflicht des *Verantwortlichen* zum Nachweis der erteilten Einwilligung.[351] Allerdings kann es hiervon Ausnahmen geben, so der EDSA: „Nachdem die Verarbeitungstätigkeit beendet wurde, sollte der Einwilligungsnachweis nicht länger aufbewahrt werden, als unbedingt zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gemäß Artikel 17 Absatz 3 Buchstaben b und e

[349] Die Einwilligung nach der Datenschutz-Grundverordnung (2021) Rz 121, https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf (abgerufen am 22.04.2022).
[350] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020, Rz 110.
[351] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020, Rz 107.

erforderlich ist."[352] Daher kann argumentiert werden, die zum Nachweis der erteilten Einwilligung verarbeiteten Daten noch für die **Dauer von bis zu einem Jahr** (relative Verjährungsfrist nach § 24 Abs 4 DSG)[353] aufzubewahren, um bei etwaigen Verfahren vor der DSB bzw vor Gericht Nachweise führen zu können. Hier ist die Wertung in der Entscheidung der DSB zur Speicherdauer von Bewerber*innendaten übernehmbar.[354]

Ein **Widerruf** der Einwilligung heißt nicht in jedem Fall, dass der *Verantwortliche* die auf dieser Grundlage verarbeiteten Daten löschen muss, wenn dieselben Daten auch für einen anderen Zweck verarbeitet werden, der nicht auf der Einwilligung der betroffenen Person beruht (zB Vertrag).[355] So führt ein **Widerruf der Einwilligung** durch die betroffene Person, so zutreffend der Bayerische Landesbeauftragte für den Datenschutz, „[…] nicht zwingend zu deren sofortiger Löschung: Mit der Verarbeitung der Einwilligung selbst wird nämlich die Nachweispflicht aus Art. 7 Abs. 1 DSGVO erfüllt; diese Verarbeitung beruht aber gerade nicht auf der Einwilligung, über die Nachweis zu führen ist."[356]

Einwilligungen im Rahmen von ID Austria: Gem § 4 Abs 5 E-GovG können (nach Maßgabe der technischen Möglichkeiten) mit Einwilligung des *E-ID-Inhabers* in die Personenbindung zusätzliche Attribute (im Gesetz als „weitere Merkmale" bezeichnet) eingefügt werden. Der *Verantwortliche* plant es Nutzer*innen freizustellen, ob die Einwilligung für den Einzelfall oder für einen längeren Zeitraum abgegeben wird:

a. Für den Einzelfall abgegebene Einwilligungen

Die einmalige Einwilligung erfolgt in der App mittels Klick auf einen Button, mit welchem die einmalige Auslieferung von Attributen an einen Service Provider freigegeben wird. Der Zweck dieser Einwilligung ist die Auslieferung von Attributen an einen Service Provider. Nach der Auslieferung der Attribute ist der Zweck der Einwilligung erfüllt, sie ist hinsichtlich weiterer Verarbeitungsvorgänge gegenstandslos geworden.

b. Längerfristig abgegebene Einwilligungen

Benutzer*innen markieren ein zusätzliches Kontrollkästchen, mit welchem sie in die längerfristige Auslieferung von Attributen an einen Service Provider (zB für ein Jahr) einwilligen, worüber diese auch entsprechend zu informieren sind. Der Zweck dieser Einwilligung ist die längerfristige Auslieferung von Attributen an einen Service Provider. Service Provider können aber nicht ohne Wissen und Zutun der

[352] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020, Rz 107 (Hervorhebung nicht im Original).
[353] „Der Anspruch auf Behandlung einer Beschwerde erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt. Verspätete Beschwerden sind zurückzuweisen."
[354] DSB 27.8.2018, DSB-D123.085/0003-DSB/2018.
[355] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020, Rz 118.
[356] Die Einwilligung nach der Datenschutz-Grundverordnung (2021) Rz 124, https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf (abgerufen am 22.04.2022).

Nutzer*innen Attribute anfordern. Benutzer*innen müssen weiterhin die Auslieferung von Attributen anstoßen und signieren. Die Einholung einer Einwilligung (Markieren eines Kontrollkästchens) fällt für die Gültigkeitsdauer der längerfristig abgegebenen Einwilligung weg, da die Verarbeitung von der längerfristig abgegebenen Einwilligung abgedeckt ist. Nach Ablauf der Gültigkeitsdauer ist eine erneute Einwilligung einzuholen.

Es gibt somit zwei Konstellationen, wie Einwilligungen erlangt werden:

- Im Fall 1 geben die Benutzer*innen die Einwilligung immer vor der Übermittlung der Attribute ab.
- Im Fall 2 geben die Benutzer*innen an, dass sie nicht mehr gefragt werden wollen, ob ein bestimmtes Attribut-Set an einen bestimmten SP übermittelt werden darf. Die Einwilligung wird also gespeichert.

In weiterer Folge stellt sich die Frage, was bezüglich der Einwilligungen (serverseitig) protokolliert und gespeichert wird.

Die erteilte Einwilligungserklärung sollte jedenfalls so lange gespeichert werden, bis diese nicht mehr gültig ist (zB bei Änderung der Verarbeitung bzw Widerruf). Darüber hinaus ist eine Speicherung mit gleichlaufenden Fristen analog zu den Protokolldaten in der ersten Phase der IDA denkbar. **Somit werden Einwilligungen derzeit idR für ein (1) Jahr ab Übermittlung gespeichert.** Bei der Weiterentwicklung der IDA-Architektur wird eine Auftrennung der Fristenläufe (für Protokolldaten und Einwilligungen) angestrebt.

Auf die **allgemeinen Anforderungen an Einwilligungen** wird im Rahmen dieses DSFA-Berichts nicht näher eingegangen; hier darf auf einschlägige Literatur verwiesen werden.[357]

4.6.7.3 Auswahl geeigneter technischer und organisatorischer Maßnahmen

Vorab ist anzumerken, dass auf Basis des risikobasierten Ansatzes der DSGVO bei (personenbezogenen) Protokolldaten entsprechend der konkreten Risikoanalyse jeweils geeignete technische und organisatorische Maßnahmen zur Risikoreduktion zu implementieren sind. Kurz gesprochen: **Je höher das (potentielle) Risiko** der Verarbeitung für die betroffenen Personen ist, **desto umfangreicher** muss **der Schutz der Protokolldaten** ausfallen.[358]

Hinsichtlich des Betriebs des E-ID Systems im BRZ kann darauf verwiesen werden, dass dort Mitarbeiter*innen regelmäßig und verpflichtend in den Themen Informationssicherheit und Datenschutz geschult werden. Zudem gibt es im BRZ diverse Sicherheitsrichtlinien, ua für den Bereich

[357] ZB *Kastelitz ua* in *Knyrim*, DatKomm Art 6 DSGVO Rz 20 ff (Stand 7.5.2020, rdb.at); siehe auch EuGH 11. 11. 2020, C-61/19, Orange România SA. Eine Checkliste findet sich auch beim Bayerischen Landesbeauftragten für den Datenschutz (2018) Rz 131; https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf (abgerufen am 22.04.2022).

[358] Siehe BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 5, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_Protokollierung.pdf?__blob=publicationFile&v=2 (abgerufen am 22.04.2022).

„Informationssicherheit am Arbeitsplatz“. Weiters werden im ID Austria Umfeld Pentests durchgeführt (letzter Testzeitraum 02/2022). Das BRZ kann schließlich verschiedene Zertifizierungen nachweisen:[359]

- IPMA-Zertifizierung: BRZ-Mitarbeiter*innen werden nach den Richtlinien der International Project Management Association (IPMA) ausgebildet. Aktuell sind im BRZ ca. 60 Mitarbeiter*innen zertifiziert.
- ISO 27001: Diese internationale Norm ermöglicht den strategischen Aufbau und die kontinuierliche Verbesserung des Informationssicherheits-Managementsystems (ISMS). Sie beschreibt die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten ISMS unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
- ISO 27018: Diese Norm legt die besonderen Pflichten eines Cloud-Anbieters fest. Damit werden vor allem die von diesen Services verarbeiteten persönlichen Daten geschützt. Externe Prüfer bestätigen die ordnungsgemäße Implementierung der neuen Norm im Rahmen des jährlichen Sicherheitsaudits.
- ISO 22301: Der aktuelle Standard ISO 22301 regelt das Business Continuity Management System. Darin sind alle proaktiven und reaktiven Maßnahmen, die die Verfügbarkeit von Informationen gewährleisten, definiert.
- ISO 9001: Diese Qualitätsmanagementnorm beschreibt Anforderungen an das Management, die Unternehmensprozesse, die Kundenorientierung und an den kontinuierlichen Verbesserungsprozess.

In concreto befinden sich seitens des *Verantwortlichen* (in Gestalt des *Auftragsverarbeiters* BRZ) zur Absicherung von Transaktions-Logdaten zusätzliche technische und organisatorische Maßnahmen in Umsetzung, die über die Standardmaßnahmen, die im BRZ bereits implementiert sind (zB OWASP Top 10), hinausgehen:

- Entwicklung eines eigenen Audit Services als Berechtigungsüberprüfung
- Datenschutz-Applikation (für BMDW) nur über SecClass 3 verfügbar (Wissen, Besitz und gesichertes Netzwerk)
- Datenschutz-Applikation kann nur über den PVP Participant des BMDWs erreicht werden, kein Public PVP
- Betriebstrennung zwischen Postgres und Audit Service (alle Mitarbeiter*innen müssen hier sicherheitsüberprüft sein)
- Datenbank Berechtigung nur Read und Write, kein Update. Delete (nach einem Jahr) wird über einen anderen Datenbank User durchgeführt > Gewährleistung der Datenintegrität / Manipulationssicherheit
- Speichern nur von Attributstypen, nicht Werten (Es wird nur „Name“ gespeichert und nicht „[Vorname] [Nachname]“)
- Lesen / Schreiben in die Datenbank nur über Audit Service - verschlüsselt

[359] https://www.brz.gv.at/was-wir-tun/sicherheit-und-qualitaet.html (abgerufen am 22.04.2022).

- Daten werden nur pseudonymisiert gespeichert (bPK)
- Konfiguration von Rate Treshholds / Throtteling (zB nur 1000 Anfragen pro Stunde), Alarming bei Überschreiten, evtl auch automatisches Disabling („Ihre Anfrage kann vorübergehend nicht beantwortet werden, bitte versuchen Sie es zu einem späteren Zeitpunkt noch einmal“)
- Authentifizierung über Client TLS zwischen allen Komponenten (Eigene Keys)
- Möglicherweise eigenen SP. Hier ist eine Neuauthentifizierung vor Zugriff notwendig, dann kann jedoch keine „Native App“ Funktionalität mehr unterstützt werden.

4.7 Datenübermittlung an Drittländer (oder internationale Organisationen)

Pseudonymisierte Daten (IP-Adresse der Benutzer*innen-Endgeräte und Push Token) werden auch in Staaten außerhalb des Europäischen Wirtschaftsraumes (EWR) verarbeitet. Dies betrifft die unten genannten *Dienstleister* Google Inc. und Apple Inc.

Für die USA hat die Europäische Kommission mit Beschluss vom 12. Juli 2016 die Entscheidung getroffen, dass unter den Regelungen des EU-US-Privacy Shields ein angemessenes Datenschutzniveau existiert (Angemessenheitsbeschluss, Art 45 Abs. 3 DSGVO). Der Europäische Gerichtshof hat am 16. Juli 2020 mit dem Urteil EuGH C-311/18 das EU-US-Privacy-Shield für unwirksam erklärt. Das Urteil kennt keine Übergangsfrist.

In seinem Urteil prüfte das Gericht auch die Gültigkeit der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (Standard Contractual Clauses, SCC) und hielt diese für gültig. Datenübermittlungen mit Google sind derzeit durch SCC gedeckt.[360]

Allerdings weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem *Datenexporteur* und dem Empfänger der Daten (dem *Datenimporteur*) die Verpflichtung auferlegt, vor jeder Übermittlung unter Berücksichtigung der Umstände der Übermittlung, zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird, und dass der *Datenimporteur* verpflichtet ist, den *Datenexporteur* über die Unfähigkeit zu informieren, die SCC und erforderlichenfalls zusätzliche Maßnahmen, zu den durch diese Klauseln gebotenen, zu erfüllen. Die Zulässigkeit der Übermittlung personenbezogener Daten in die USA auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall ab, wobei die Umstände der Übermittlung und zusätzlich ergriffene Maßnahmen zu berücksichtigen sind.

Um einerseits die bestehenden alten SCC aus 2001 bzw 2010 an die DSGVO anzupassen, und andererseits den zwischenzeitlich konkretisierten Anforderungen des EuGH an Drittstaatstransfers nachzukommen, hat die Europäische Kommission am 4. Juni 2021 neue SCC für die Übermittlung personenbezogener Daten an Drittländer beschlossen.

Die neuen SCC decken dabei durch einen „modularen Ansatz“ eine breite Palette von Übermittlungsszenarien ab (anstelle separater Klauseln, die bislang nicht alle denkbaren Szenarien vorsahen) und sehen nunmehr die Möglichkeit für *Dritte* vor, zwischen zwei Parteien bereits abgeschlossenen Standardvertragsklauseln beizutreten. Darüber hinaus enthalten die SCC einen Überblick über die Schritte, die Unternehmen ergreifen müssen, um dem Schrems-II-Urteil nachzukommen,[361] sowie Beispiele für mögliche „ergänzende Maßnahmen“ zur Sicherstellung eines angemessenen Datenschutzniveaus.

Die neuen SCC wurden am 7. Juni 2021 im Amtsblatt der EU veröffentlicht, treten am 27. Juni 2021 in Kraft und sind spätestens ab dem 27 September 2021 zwingend für alle Neuverträge zu verwenden. Spätestens bis zum 27. Dezember 2022 müssen alle Altverträge, die auf der Grundlage der bisherigen SCC abgeschlossen wurden, auf die neuen SCC umgestellt worden sein. Aufgrund der zahlreichen

[360] Für Google Firebase Services siehe: https://firebase.google.com/terms/data-processing-terms (abgerufen am 22. 04. 2022)
[361] Siehe EuGH 16. Juli 2020, C-311/18, Facebook Ireland und Schrems.

Änderungen und Ergänzungen in den neuen SCC, die bereits auf das Schrems II-Urteil Rücksicht nehmen, ist die Verwendung der alten SCC nicht zu empfehlen.

In diesem Zusammenhang ist darauf hinzuweisen, dass aufgrund der vorgenommenen Verschlüsselung der Daten eine Identifizierung von betroffenen Personen durch den *Auftragsverarbeiter* nicht vorgenommen werden kann. Solche Informationen sind auch nicht aus dem Verarbeitungskontext ableitbar.

Die App bindet bestimmte Technologien (sogenannte Software Development Kits, SDK) ein, um die Nutzung bestimmter Funktionen der App zu gewährleisten bzw zu verbessern. In diesem Zusammenhang werden Firebase-Messaging Dienste von Google eingesetzt, um Push Benachrichtigungen an Nutzer*innen zu übermitteln. Dabei werden Daten (IP-Adresse) verarbeitet und an den Anbieter (Google) übermittelt. Der *Verantwortliche* hat eine Marktumschau durchgeführt und festgestellt, dass es keine belastbaren Alternativprodukte gibt. Die Nutzung von Google FCM erscheint derzeit sohin alternativlos. Der *Verantwortliche* wird den Markt auch zukünftig beobachten und ggf auf entsprechende Alternativlösungen setzen.

Die Umsetzung der Push Benachrichtigung erfordert für die App auf den mobilen Endgeräten nämlich die Einbindung des Dienstes Google Firebase Messaging - einer der weltweit verbreitetsten Services, der bei der überwiegenden Zahl aller Apps im Hintergrund läuft, und zwar auf den Systemen aller Hersteller*innen, nicht nur auf Google Android Geräten. Dieser Dienst erfordert in geringem Umfang, dass eine Kommunikation zwischen dem Endgerät und dem Server des Firebase Dienstes (von Google) stattfindet, etwa initial, weil ein Token zugewiesen wird, über den in der Folge ohne Nutzer*innen- oder Gerätebezug der Dienst im Hintergrund seine Aufgabe erfüllen kann. Hier erfolgt auch eine Übertragung der IP-Adresse des Endgeräts, allerdings nur einmalig und nicht laufend, soweit es nur den Dienst der firebase-push-notifications betrifft. Die Nutzungsbedingungen des *Auftragsverarbeiters* Google umfassen auch Regelungspunkte des Art 28 DSGVO.[362]

Allerdings besteht hier ohne nähere Aufmerksamkeit das Risiko, dass zugleich auch der – standardmäßig aktivierte – Zusatzdienst Firebase Analytics eingeschaltet ist, weil damit ohne weiteren Programmieraufwand die Statistik über die Nutzung des Push Services erfasst werden kann. Ein aus Sicht des Betroffenenrisikos unerwünschter Nebeneffekt ist dabei jedoch, dass sich der Datenaustausch im Hinblick auf Häufigkeit und Menge zwischen dem Endgerät und dem Google-Backend signifikant erhöht und dabei das Risiko entsteht, dass Google damit deutlich mehr Informationen über die Nutzung der App sowie allenfalls über Auslandsaufenthalte der Nutzer*innen erhält. Im Zuge der Entwicklung wurde daher durch das Datenschutzteam beauftragt, die Google Firebase Analytics Dienste konsequent zu deaktivieren. Die Deaktivierung von Firebase Analytics wurde durch das BMDW bestätigt.

Im Hinblick auf die sorgfältige Datenminimierung und die Umsetzung von „Datenschutz durch Technik“ ist im konkreten Fall festzustellen, dass durch die eingeschränkte Verarbeitung pseudonymisierter Daten keine hohen zusätzlichen Risiken für die Rechte und Freiheiten der Betroffenen erwachsen.

[362] Siehe https://firebase.google.com/terms/data-processing-terms (abgerufen am 22. 04. 2022).

Im Lichte der Entscheidungspraxis der österreichischen Datenschutzbehörde[363] ist die Zulässigkeit der Datenübermittlung auf Basis der SCC dennoch zu hinterfragen.[364] Im Hinblick auf die Nutzung von Firebase Cloud Messaging sind demnach keine Maßnahmen erkennbar, welche die anfallende Kommunikation entsprechend schützen.

Als Rechtsgrundlage für die Drittlandsübermittlung kommt daher insbesondere Art 49 Abs 1 lit a DSGVO in Frage, nach dem eine Übermittlung in ein Drittland zulässig ist soweit eine ausdrückliche Einwilligung der betroffenen Person eingeholt wurde.[365] Die einwilligende Person ist vorher auf die Risiken einer derartigen Datenübermittlung hinzuweisen; es ist also ein Gefahrenhinweis erforderlich, welcher dem Erfordernis einer informierten Einwilligung Rechnung trägt und kumulativ zu den Anforderungen der Art 4 Z 11 und Art 7 und 8 hinzutritt.[366]

Im Zusammenwirken mit dem ID Austria System übermitteln folgende Dienstleister*innen personenbezogene Daten in Drittländer:

Google Inc. Mountain View, 1600 Amphitheatre Parkway, CA 94043 United States [367]

Kurzbeschreibung der Verarbeitungstätigkeiten: Die Benachrichtigung über eine Signatur wird mit Hilfe des Firebase Cloud Messaging Services realisiert. Um den Versand von Push Benachrichtigungen zu ermöglichen, wird beim Erst-Start der App ein Firebase Cloud Messaging Registration Token erstellt, welcher die App-Installation auf dem Gerät eindeutig identifiziert. Der Token dient zum Erkennen des Nachrichtenziels.

Apple Inc., 1 Apple Park Way Cupertino, CA 95014 United States[368]

Kurzbeschreibung der Dienstleistung: Das Apple Notification Service erhält von Firebase Cloud Messaging (FCM) Anfragen zum Versand von Push Benachrichtigungen an iOS Benutzer*innen. Die Push Benachrichtigung enthält keine empfänger*innenspezifischen und damit personenbezogenen Daten. Für die Zustellung (Network Layer) wird auf der Basis des Betriebssystems die IP-Adresse des Geräts verarbeitet. Diese Verarbeitungstätigkeit wird im Zuge der allgemeinen Betriebssystemkommunikation abgewickelt. Die Applikation ruft in dieser Hinsicht keine zusätzlichen Verarbeitungen personenbezogener Daten hervor. Deshalb liegt aus Sicht der Applikation keine Auftragsverarbeitung zu Apple vor.

[363] DSB, 22.12.2021, D155.0272021-0.586.257.
[364] DSB, 22.12.2021, D155.0272021-0.586.257.
[365] Zu beachten ist, dass dies lt EDSA nur für gelegentliche Übermittlungen gedacht ist; vgl EDSA, „Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung 2016/679“ (Stand: 25.5.2018, „Leitlinien 2/2018“), unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf (abgerufen am 22. 04. 2022); beachte die (begründete) ggt Ansicht von *Kremer/Christmann-Thoma/Kamm/Matejek/Schneider*, Datentransfer nach Art. 49 DSGVO: Was geht, wenn sonst nichts geht?, CR 12/2021. D 784 ff.
[366] Vgl *Knyrim* in *Knyrim*, DatKomm (2019) Art 49 Rz 17.
[367] Die Nutzung von Firebase unterliegt automatisch den Richtlinien von Google, die auch einen AVV enthalten: https://firebase.google.com/terms/data-processing-terms (abgerufen am 22. 04. 2022).; für weitere Informationen zu Google Firebase Cloud Messaging siehe unter https://firebase.google.com/products/cloud-messaging/ (abgerufen am 22. 04. 2022); siehe zudem die Datenschutzerklärung http://www.google.de/intl/de/policies/privacy sowie die Firebase-Datenschutzerklärung unter https://firebase.google.com/support/privacy (abgerufen am 22. 04. 2022).
[368] Siehe https://www.apple.com/legal/privacy/ (abgerufen am 22. 04. 2022).

4.8 Rat des *Datenschutzbeauftragten* und Standpunkt der Betroffenen

Nach Art 35 Abs 2 DSGVO hat der *Verantwortliche* bei Durchführung einer DSFA den Rat des *Datenschutzbeauftragten* einzuholen. Ob der Rat des *Datenschutzbeauftragten* verpflichtend einzuholen ist und inwiefern dem eingeholten Rat zu folgen ist, wird in der Literatur uneinheitlich kommentiert. *Trieb* geht bspw davon aus, dass die DSGVO keine solche Pflicht statuiert;[369] *Jandt* sieht in der Bestimmung wiederum eine Pflicht, die Vorschrift treffe jedoch keine Aussage darüber, ob dem Rat des *Datenschutzbeauftragten* auch zu folgen sei und sehe für diesen auch kein Vetorecht oder ähnliches vor.[370] Falls der *Verantwortliche* mit dem vom *Datenschutzbeauftragten* eingeholten Rat (oder Teilen davon) nicht einverstanden ist, sollte nach Ansicht der Art-29-Datenschutzgruppe jedoch eine (nachvollziehbare) Begründung für die mangelnde Beachtung des Ratschlags in den DSFA-Bericht aufgenommen werden.[371]

Im vorliegenden Fall wird die Konsultierung der *Datenschutzbeauftragen* jedenfalls als sinnvoll erachtet. Die Einbindung der *Datenschutzbeauftragten* des BMDW erfolgte zunächst über die internen Kommunikationswege des Ministeriums; auf diese Weise wurde über den Fortschritt und die wesentlichen Inhalte durchgehend informiert. Mitte Februar 2022 wurde ein Zwischenstand des Dokuments zur Sichtung an die *Datenschutzbeauftragten* des BMDW übermittelt. Ende Februar 2022 fand ein Abstimmungstermin zwischen dem Research Institute, den *Datenschutzbeauftragten* sowie weiteren Mitarbeiter*innen des BMDW zu wesentlichen inhaltlichen Punkten und der weiteren Form der Einbindung statt. Die *Datenschutzbeauftragten* legten in diesem Termin eine transparente Einbindung durch den *Verantwortlichen* nachvollziehbar dar. Die internen *Datenschutzbeauftragten* des BMDW haben folgendes zum übermittelten Zwischenstand der DSFA angemerkt:

- Die quantitative Darstellung des Risikos anhand einer Risikomatrix wird begrüßt;
- Die materiell-rechtlichen Rechtsgrundlagen werden als gut eingebunden und die Schwellwertanalyse als präzise durchgeführt erachtet;
- Die technischen und organisatorischen Maßnahmen der Risikoanalyse sollen in der weiteren Vorgehensweise möglichst konkret und präzise beschrieben werden;
- Schließlich erklären sich die *Datenschutzbeauftragten* dazu bereit auch weiterhin als Schnittstelle zwischen Research Institute und BMDW zu Verfügung zu stehen; diesbezüglich wird festgehalten, dass die internen *Datenschutzbeauftragten* des BMDW laufend über den Projektfortschritt unterrichtet werden.

Darüber hinaus ist im Zuge einer DSFA gem Art 35 Abs 9 DSGVO gegebenenfalls der Standpunkt der betroffenen Personen oder ihrer Vertreter*innen einzuholen.[372] Die Bestimmung des Abs 9 schafft grundsätzlich die Möglichkeit, die individuelle Meinung einzelner Betroffener in Erfahrung zu

[369] Vgl *Trieb* in *Knyrim*, DatKomm (2019) Art 35 Rz 124.
[370] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG (2018) Art 35 Rz 18.
[371] So die Art-29-Datenschutzgruppe, WP 243 rev. 01, 17 unter Hinweis auf Art 24 Abs 1 DSGVO.
[372] Siehe hierzu auch Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01 (2017) 28 f.

bringen.[373] Alternativ können auch deren Vertreter*innen herangezogen werden, wobei in erster Linie an verschiedene Interessensvertretungen, Betriebsräte oder Verbraucher*innenschutzverbände zu denken ist. Der Standpunkt dieser Einrichtungen sollten insb dann berücksichtigt werden, wenn die beabsichtigte Datenverarbeitung eine große Zahl betroffener Personen erfasst, deren Interessen der jeweilige Verband oder die jeweilige Stelle vertritt.[374] Auch diese Regelung lässt in mehrfacher Hinsicht Deutungsspielräume offen.[375] Unklarheiten bestehen bspw hinsichtlich des Stellenwerts des Standpunkts der betreffenden Stellen für die Einbeziehung in den Prüfprozess der DSFA. Die Formulierung "gegebenenfalls" lässt zudem offen, unter welchen Umständen der Standpunkt einzuholen ist und wann darauf verzichtet werden kann.[376] Eine bedingungslose Verpflichtung für *Verantwortliche* zur Einholung wird auf Basis dieser Bestimmung nicht unterstellt werden können;[377] die jeweilige Vorgehensweise ist jedoch zu dokumentieren bzw zu begründen.[378]

Stellvertretend für die Betroffenen wird im vorliegenden Fall der Standpunkt verschiedener einschlägiger Interessensvertretungen und NGOs berücksichtigt; zudem wird auf die politische Debatte zum E-GovG und internationale Studien mit weiterführenden Vorschlägen für die sicherheitstechnisch robuste und rechtskonforme Implementierung staatlicher E-ID Systeme eingegangen.[379] Auf diese Weise wird der öffentliche Diskurs zur Thematik abgebildet und in die DSFA miteinbezogen. Dies soll dazu dienen, frühzeitig Erkenntnisse über Erwartungen und Prioritäten von Betroffenen und anderen gesellschaftlichen Akteur*innen zu liefern.[380]

So berichtet die Parlamentsdirektion 2017, dass in der Behandlung des E-GovG vonseiten der SPÖ die Benutzer*innenfreundlichkeit und technische Sicherheit des E-ID Systems als oberste Prämisse betont wurde; es solle daher „[...] ein transparentes Protokoll geben [...], um selbst nachsehen zu können, was protokolliert wurde"; zudem wird vonseiten der Opposition gefordert „eine zentrale Protokollierung auszuschließen".[381]

Weiters hat die Grundrechtsplattform epicenter.works zur E-ID im Jahr 2020 ua folgende Positionen vertreten:[382]

- Es wird ein dezentrales und unbeobachtbares Identitätssystem gefordert bzw befürwortet; einzelne Ausweis- oder Login-Vorgänge dürfen nicht in einer zentralen Datenbank erfasst

[373] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.
[374] Vgl *Trieb* in *Knyrim*, DatKomm (2019) Art 35 Rz 134; Vgl hierzu auch *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38 ff.
[375] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff;
[376] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff; In der englischen Version der DSGVO wird bspw die Formulierung „where appropriate" verwendet; vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 131.
[377] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 131.
[378] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG (2018) Art 35 Rz 58.
[379] Um die Thematik angemessen zu adressieren kann die Einholung des Standpunkts der Betroffenen künftig auch über den Datenschutzrat oder repräsentative demoskopische Erhebungen erfolgen. Ebenso wäre eine systematische Durchführung und Auswertung qualitativer Gespräche mit Betroffenen zu deren Sichtweisen erhellend; so bspw, wenn es um die Beurteilung angemessener Informationspflichten und datenschutzrechtliche Transparenzkriterien geht. Insb zur Beleuchtung sicherheitskritischer Aspekte scheint in der methodischen Weiterführung der DSFA auch die Durchführung von Fokusgruppen sinnvoll; siehe methodisch weiterführend *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 25 ff.
[380] *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 25 ff.
[381] Siehe https://www.ots.at/presseaussendung/OTS_20170629_OTS0397/elektronischer-identitaetsnachweis-e-id-wird-neue-buergerkarte (abgerufen am 22. 04. 2022).
[382] Siehe https://epicenter.works/content/unsere-position-zur-elektronischen-identitaet (abgerufen am 22.04.2022).

werden; die Schaffung einer entsprechenden Architektur unter Verwendung kryptographischer Pseudonyme, die „Unlinkability“ garantieren, wird gefordert.[383]

- Weiters wird gefordert, dass der Zugriff privater Unternehmen eine starke Kontrolle der Use Cases braucht und die Prinzipien der Datensparsamkeit und strengen Zweckbindung umzusetzen sind.
- Diese Software muss weiters quelloffen und bestenfalls unter freier Lizenz veröffentlicht sein, damit alles nachvollziehbar ist und Menschen mit freien Betriebssystemen nicht ausgeschlossen werden.
- Es muss ein einfach zugängliches (wenn möglich User-seitig gespeichertes) Verzeichnis aller Zustimmungen sowie die Möglichkeit des Widerrufs und der Beauskunftung der Daten geben.
- Schließlich wird gefordert, dass der E-ID das Prinzip der anonymen Nutzung von technischen Infrastruktursystemen nicht untergraben darf.

Die Organisation verweist zudem auf das Missbrauchspotential des Systems und Formen von (staatlicher) Überwachung;[384] zudem wird davon ausgegangen, dass das zentralisierte E-ID System zugleich einen sicherheitstechnischen Angriffspunkt schafft. Hinsichtlich der Verflechtung mit den diversen Anwendungen und (privaten) Service Providern wird auch eine künftige Verbindung der ID Austria mit der App „Grüner Pass“ als denkbar erachtet.[385]

Der Datenschutzrat hat in seiner Stellungnahme vom 28. September 2020 zur Novelle des E-GovG 2020 unter anderem folgende Positionen vertreten:[386]

- Bei der Verwendung biometrischer Merkmale handelt es sich um eine Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art 9 DSGVO und eine alternative Nutzung ohne Verwendung besonderer Datenkategorien soll daher ermöglicht werden.
- Soweit im Zusammenhang mit dieser Verarbeitung auf Verarbeitungsergebnisse *Dritter* (zB Betriebssystemhersteller, Hersteller von Mobilgeräten) zurückgegriffen wird, soll einerseits die Sicherheit derartiger Verarbeitungen überprüft werden und geklärt werden, ob es sich dabei um eine Auftragsverarbeitung handelt bzw auf Basis welcher anderen Rechtsgrundlage die Datenbereitstellung erfolgt sowie, ob es im Zuge dieser Datenverarbeitungen zu Datenübermittlungen in Drittstaaten, wie insbesondere die USA, erfolgen.
- In Bezug auf die Einwilligung in die Einbindung weiterer Merkmale (erwähnt ua in § 4 Abs 5 E-GovG) soll, zB durch einen Verweis auf Art 4 Z 11 DSGVO, klargestellt werden, ob die

[383] Siehe zB *Hölzl/Roland/Mayrhofer*, Real-World Identification for an Extensible and Privacy Preserving Mobile eID, in *Hansen/Kosta/Navi-Foviono/Fischer-Hübner* (Hrsg) Privacy and Identity Management – The Smart Revolution (2018) 354 ff; https://link.springer.com/chapter/10.1007/978-3-319-92925-5_24 (abgerufen am 22. 04.2022).
[384] Siehe https://epicenter.works/content/unsere-position-zur-elektronischen-identitaet; siehe zu Frage der Überwachung durch staatliche ID Systeme weiterführend auch *Boersma et al*, Histories of State Surveillance in Europe and Beyond (2014) 133 ff; von den Autoren wird bspw ein historischer Zusammenhang von E-ID Systemen mit autoritären Regimen in Spanien, Portugal, Belgien und den Niederlanden aufgezeigt.
[385] Siehe https://futurezone.at/digital-life/digitaler-ausweis-id-austria-fuehrerschein-handy-signatur-buergerkarte/401480884 (abgerufen am 22. 04.2022).
[386] Siehe *Datenschutzrat*, Stellungnahme vom 28.09.2020 zum Entwurf eines Bundesgesetzes, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden, GZ 2020-0.623.605; https://www.bmj.gv.at/dam/jcr:4e4f61fb-afb7-4c83-b6e4-09b98a42d4ca/ERL_I_Stellungnahme_des_Datenschutzrates.pdf (abgerufen am 22. 04.2022).

Einwilligung des *E-ID-Inhabers* auch eine datenschutzrechtliche Einwilligung gemäß Art 4 Z 11 DSGVO darstellt und demzufolge an die diesbezüglichen unionsrechtlichen Voraussetzungen gebunden ist.

- Es soll geregelt werden (in § 4a Abs 4 E-GovG), wie lange die von der Behörde eingeholten Informationen und Dokumente zu speichern sind. Im Lichte der Grundsätze der Datenminimierung und Speicherbegrenzung sowie insbesondere des Verhältnismäßigkeitsgrundsatzes soll zudem deutlich klarer geregelt werden, welche personenbezogenen Daten in diesen Informationen und Dokumenten verarbeitet werden und wozu eine derart weitreichende Befugnis der Behörde zur Einholung von Informationen und Dokumenten nur für die Identitätsfeststellung unbedingt erforderlich ist.
- Im Hinblick auf die Anforderungen gemäß Art 23 Abs 2 DSGVO an eine Gesetzgebungsmaßnahme wie jene des § 4b Abs 2 E-GovG (kein Widerspruchsrecht gemäß Art 21 DSGVO sowie kein Recht auf Einschränkung der Verarbeitung gemäß Art 18 DSGVO) ist diese Bestimmung zu präzisieren.
- Zuverlässigkeitsüberprüfungen von *Dritten*, denen die Nutzung des E-ID Systems eröffnet wird, sind grundsätzlich notwendig. Hinsichtlich möglicher Anfragen an die Datenschutzbehörde, ob und über welche Anhaltspunkte sie verfügt, dass der *Dritte* in den letzten fünf Jahren personenbezogene Daten nicht auf diese Weise verarbeitet hat, wird festgehalten, dass die (unabhängige) Datenschutzbehörde diese Daten nicht für diese Zwecke erhoben hat bzw verarbeitet (gemeint offenbar im Sinne einer Art Verwaltungsstrafregister für Datenschutzverstöße, wofür jedoch eine gesetzliche Grundlage fehlt). Zudem steht diese Anfrage in einem evidenten Spannungsverhältnis mit der Unabhängigkeit der Datenschutzbehörde [Anm.: Eine derartige Bestimmung scheint daher im Gesetzgebungsprozess entfallen zu sein].
- Auch für die im Pilotbetrieb verarbeiteten personenbezogenen (Echt-)Daten sind die Vorgaben der DSGVO und des DSG – etwa hinsichtlich der erforderlichen Rechtsgrundlagen – vollumfänglich anzuwenden.
- Zudem wurden einige spezifische Konkretisierungen im Gesetz gefordert.

Mit Bezug auf Deutschland übt wiederum der Chaos Computer Club (CCC) Kritik an der strategischen Umsetzung der Implementierung des E-ID. Der Verein verweist aber auch auf enorme Netzwerkeffekte, die das System haben könnte. Von dieser Warte aus wird auch der fehlende Zugang zu sicheren und erschwinglichen Endgeräten für die breite Bevölkerung thematisiert.[387] Zugleich wird die Vermischung von hoheitlichen Identifizierungsaufgaben mit den Erfordernissen der Wirtschaft zur Identifizierung im Rechtsverkehr als problematisch erachtet.[388] Der CCC verweist in seiner Stellungnahme darüber hinaus auf Alternativen, wie das von der weltweiten Mobilfunk-Vereinigung GSMA spezifizierte Mobile Identity System.

[387] Vgl https://www.ccc.de/de/updates/2021/gemeinsame-stellungnahme-zum-eid-gesetz-entwurf (abgerufen am 22. 04.2022).
[388] Vgl https://www.ccc.de/system/uploads/225/original/ccc-stellungnahme-eID.pdf (abgerufen am 22. 04.2022).

In internationaler Hinsicht kann auch auf einen Bericht von Privacy International verwiesen werden; in diesem werden digitale ID Systeme in Verbindung mit der Problematik der False Positives im Bereich der biometrischen Identifikation thematisiert.[389] So wird mit Bezug auf die Unique Identification Authority of India (UIDAI) eine False Positive Identification Rate von 0.0025% bzw 2,5 False Positives auf 100.000 Fälle berichtet.

Weiterführend sei hier zudem auf Berichte bzw Stellungnahmen von McKinsey sowie der Weltbank verwiesen. Wenngleich es sich hierbei nicht mehr um Einrichtungen bzw Institutionen handelt, die unmittelbar als Vertreterinnen der Betroffenen bezeichnet werden können, liefern deren Studien bzw Stellungnahmen ergänzende Einsichten und Ansatzpunkte. So nimmt das McKinsey Global Institute in einer Studie Bezug auf die staatlichen ID Systeme in Brasilien, China, Äthiopien, Indien, Nigeria, Großbritannien sowie den USA und hebt den „potential economic impact" der ID Systeme hervor.[390] Dabei wird die Ansicht vertreten, dass E-ID Systeme trotz der verschiedenen Risiken „a powerful key to inclusive growth" sein können;[391] im Ergebnis werden diese als „new frontier in value creation for individuals and institutions around the world" bezeichnet.[392]

Neben ökonomischen Aspekten zeigt McKinsey jedoch auch eine Reihe an Risiken auf. Es handelt sich diesbezüglich überwiegend um Aspekte der technischen Infrastruktur und Datensicherheit (Cybersecurity Threats) die üblicherweise im Zusammenhang mit „digital technologies with large-scale population-level usage" vorkommen. Dabei geht es um technisches Versagen einer systemrelevanten Infrastruktur ebenso wie die missbräuchliche Verarbeitung von Daten. Im Kern wird die Ansicht vertreten, dass die Implementierung digitaler ID Systeme folgende Risiken impliziert:[393]

- Cybersecurity-Bedrohungen stellen ein wachsendes Risiko im gesamten digitalen Ökosystem dar; digitale ID Systeme sind hier keine Ausnahme.
- Die digitale ID wird dem Risiko von Fehlverhalten durch Mitarbeiter*innen der ID-Anbieter*innen ausgesetzt sein.
- Die unbefugte Verwendung oder Manipulation von Zugangsdaten stellt ein Risiko der digitalen ID dar; auch im Fall der Verarbeitung biometrischer Merkmale.
- Digitale IDs bergen, wie zuvor konventionelle IDs, das Risiko, Einzelpersonen von der Nutzung auszuschließen; „[...] individuals without sufficient technological access or savvy and those who do not trust a digital ID system could be completely excluded, unless alternative manual options also exist."[394]

Auch die Weltbank bezeichnet die Implementierung staatlicher E-ID Systeme – ähnlich wie McKinsey – als Möglichkeit zur nachhaltigen Entwicklung und verweist dabei auf den Zugang zu Gesundheits-

[389] Vgl https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms (abgerufen am 22. 04.2022).
[390] *White* et al; Digital identification: A key to inclusive growth; McKinsey Global Institute (2019).
[391] *White* et al; Digital identification: A key to inclusive growth; McKinsey Global Institute (2019): „[...] full digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030, with just over half of the potential economic value potentially accruing to individuals."
[392] *White* et al; Digital identification: A key to inclusive growth; McKinsey Global Institute (2019).
[393] *White* et al; Digital identification: A key to inclusive growth; McKinsey Global Institute (2019) 77 ff.
[394] *White* et al; Digital identification: A key to inclusive growth; McKinsey Global Institute (2019) 77 ff (83).

und Bankensystemen in Thailand, Pakistan, Peru und Indien.[395] Für die Schaffung robuster staatlicher ID Systeme wird in der Stellungnahme die Berücksichtigung und Anwendung der folgenden zehn Prinzipien empfohlen:[396]

- „Ensuring universal coverage for individuals from birth to death, free from discrimination.
- Removing barriers to access and usage and disparities in the availability of information and technology.
- Establishing a robust - unique, secure and accurate - identity.
- Creating a platform that is interoperable and responsive to the needs of various users.
- Using open standards and ensuring vendor and technology neutrality.
- Protecting user privacy and control through system design.
- Planning for financial and operational sustainability without compromising accessibility.
- Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
- Establishing clear institutional mandates and accountability.
- Enforcing legal and trust frameworks though independent oversight and adjudication of grievances."

Die verschiedenen Standpunkte der Interessensvertretungen, Verbände und Institutionen werden in weiterer Folge in der Technikfolgen- und Risikoabschätzung berücksichtigt. Aus methodischer Sicht soll dies dazu beitragen die Akzeptanz der Technologie zu fördern und das Risiko unerwarteter und unkontrollierbarer Ablehnung seitens der Betroffenen oder sonstiger gesellschaftlicher Akteur*innen zu minimieren.[397]

[395] Vgl https://blogs.worldbank.org/digital-development/ten-principles-identification-sustainable-development (abgerufen am 22. 04. 2022).
[396] Vgl https://blogs.worldbank.org/digital-development/ten-principles-identification-sustainable-development (abgerufen am 22. 04. 2022).
[397] Vgl *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 25 ff.

5 Datenschutzrechtliche Risikoabschätzung – Risk Assessment

Aus Art 35 Abs 7 lit c DSGVO ergibt sich für die ordnungsgemäße Durchführung einer DSFA die rechtliche Anforderung zur "Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen". Während die Formulierung "Rechte und Freiheiten natürlicher Personen" primär auf die Ziele der DSGVO gem Art 1 Abs 2 referenziert,[398] ist der Begriff „Risiko" in der DSGVO nicht ausdrücklich definiert. Aus ErwGr 75 und 94 DSGVO lässt sich ableiten, dass ein Risiko als das Bestehen der Möglichkeit des Eintritts eines Ereignisses verstanden wird, das selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.[399] Zudem lässt sich den Erwägungsgründen entnehmen, dass datenschutzrechtliche Risiken grundsätzlich nach "Eintrittswahrscheinlichkeit" und "Schwere" zu beurteilen sind. Weiters wird zwischen "physischen", "materiellen" und "immateriellen" Schäden unterschieden.[400] Dabei werden exemplarisch die folgenden Szenarien angeführt:

- Diskriminierung
- Identitätsdiebstahl oder -betrug
- Finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
- Unbefugte Aufhebung der Pseudonymisierung

Zudem wird auf andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile verwiesen, die entstehen können,

- wenn betroffene Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- wenn besondere Kategorien von personenbezogenen Daten verarbeitet oder persönliche Aspekte (wie insb Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel) bewertet, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen (insb von Kindern), verarbeitet werden oder
- wenn die Verarbeitung eine große Menge an personenbezogenen Daten und eine große Anzahl von Personen betrifft.

[398] Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG (2018) Art 35 Rz 42. Siehe weiterführend auch die Gewährleistungsziele der DSGVO: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Intervenierbarkeit, Nichtverkettbarkeit und Transparenz in *Martin* et al, Datenschutz-Folgenabschätzung (2020) 55 ff.
[399] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38; vgl *European Data Protection Supervisor (EDPS)*, Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 8.
[400] Vgl ErwGr 75 DSGVO. Siehe auch *Martin* et al, Datenschutz-Folgenabschätzung (2020) 39 f.

Weitere exemplarisch angeführte Bedrohungsszenarien für den Bereich der IT-Sicherheit können ua dem IT-Grundschutz-Katalog des deutschen Bundesamts für Sicherheit in der Informationstechnik entnommen werden.[401]

Unter Bezugnahme auf die projektspezifische Abgrenzung und BMDW-seitige Schwerpunktsetzung geht es im Folgenden nicht um eine abschließende Beurteilung sämtlicher möglicher Risiken, sondern zunächst nur um die Analyse jener datenschutzrechtlicher Risikoszenarien, die in Verbindung mit den vier herausgestellten Verarbeitungsprozessen des ID Austria Systems stehen bzw aus diesen hervorgehen können.[402] Besonderes Augenmerk wird dabei auf die Aufzeichnung, Einsicht und Aufbewahrung von Transaktions-Logs sowie die mit der Verwendung des ID Austria Systems in Zusammenhang stehenden Einwilligungserklärungen gelegt.

Da die DSFA in rechtlicher wie methodischer Hinsicht als laufendes Self-Assessment zu sehen ist, stellt die im Folgenden dargelegte Risikobeurteilung für die *Verantwortlichen* zugleich eine methodische Grundkonzeption dar, die im Zuge des Betriebs des ID Austria Systems laufend weitergeführt werden kann und soll.

Sollten sich die Datenverarbeitungsprozesse oder das Risikoumfeld ändern, ist jedenfalls zu überprüfen, ob die DSFA noch der Realität entspricht und bei Bedarf eine Aktualisierung vorzunehmen.[403]

[401] Siehe https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf (abgerufen am 22. 04. 2022).
[402] Siehe hierzu insb Kapitel 3.2.
[403] Vgl *European Data Protection Supervisor (EDPS)*, Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 6.

5.1 Methodologie

Die Methodik der nachfolgenden Risikobeurteilung stützt sich im Kern auf die Risk Management ISO-Norm 31000:2018.[404] Darüber hinaus wurde Anleihe am Risk Assessment Leitfaden des deutschen Bundesverbands der Informationswirtschaft, Telekommunikationsbranche (Bitkom),[405] sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Fraunhofer-Institutes für System- und Innovationsforschung genommen.[406]

Der Europäische Data Protection Supervisor (EDPS) sieht grundsätzliche keine spezifische Methode zur Durchführung einer DSFA vor, sondern erachtet jede Vorgehensweise für zulässig, die im Einklang mit den Vorschriften der DSGVO und den Leitlinien der Artikel-29-Datenschutzgruppe steht.[407]

Die Artikel-29-Datenschutzgruppe empfiehlt für die Durchführung einer Risikobeurteilung, mit Verweis auf Art 35 Abs 7 sowie ErwGr 84 und 90 der DSGVO, insb [408]

- Ursache, Art, Besonderheit und Schwere jedes einzelnen Risikos aus Sicht der Betroffenen zu bewerten, (indem Risikoquellen berücksichtigt, potenzielle Auswirkungen und Bedrohungen auf die Rechte und Freiheiten von Betroffenen ermittelt und deren Eintrittswahrscheinlichkeit und Schwere bewertet werden).
- Zudem sollen Maßnahmen zur Bewältigung dieser Risiken ermittelt werden.[409]

In ErwGr 83 wird weiter ausgeführt, dass bei der Bewertung der Datensicherheitsrisiken insb Szenarien wie Vernichtung, Verlust, Veränderung oder eine unbefugte Offenlegung von bzw ein unbefugter Zugang zu personenbezogenen Daten zu berücksichtigen sind.[410]

In den methodischen Ausführungen des Frauenhofer-Instituts werden für die generelle Erfassung eines Risikoszenarios wiederum die folgenden übergeordneten Fragen aufgeworfen:[411]

- Welche Schäden können für betroffene Personen auf Grundlage der geplanten Datenverarbeitung auftreten?
- Durch welche Handlungen bzw Umstände kann es zum Eintritt der jeweiligen Schadensereignisse kommen? Welche Akteur*innen bzw (nicht-menschliche) Risikoquellen sind dabei wie involviert?

[404] https://www.iso.org/standard/43170.html (abgerufen am 22.04.2022).
[405] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017).
[406] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38 ff; siehe zudem weiterführend Art-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01 (4. Oktober 2017); siehe auch European Data Protection Supervisor (EDPS), Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 5 ff.
[407] Vgl *European Data Protection Supervisor (EDPS)*, Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 6.
[408] Siehe *Artikel 29 Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01 (2017) 28 f.
[409] Siehe Art 35 Abs 7 lit d sowie ErwGr 84 und 90 DSGVO.
[410] Vgl ErwGr 83 DSGVO.
[411] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 43.

– Welche Abhilfemaßnahmen sind bereits implementiert bzw geplant?[412]

Unter Bezugnahme auf die Vorgaben der DSGVO und die verschiedenen methodischen Leitfäden und Empfehlungen für die Durchführung einer DSFA, lässt sich der Prozess der Risikobeurteilung generisch in die folgenden methodischen Teilschritte untergliedern:[413]

– **Risikoidentifikation:** Beschreibung des Szenarios, Ermittlung beteiligter Akteur*innen und betroffener Personen, Bestimmung der Ursache und Ermittlung der auslösenden Risikoquelle, Feststellung des möglichen Schadens im Hinblick auf tangierte Gewährleistungsziele der DSGVO)

– **Risikoanalyse und -bewertung:** Bestimmung der Eintrittswahrscheinlichkeit und Schwere des Schadens, Klassifizierung bzw Bewertung des Risikoszenarios anhand einer Risikomatrix in hoch, normal oder gering bzw akzeptabel oder nicht-akzeptabel

– **Risikobehandlung:** Berücksichtigung bestehender technischer und organisatorischer Maßnahmen der Risikomitigierung, Bestimmung von Abhilfemaßnahmen zur Minimierung identifizierter Risiken, neuerliche Risikobewertung

Zum Prozess der Beurteilung wird in ErwGr 76 zudem ausgeführt, dass Eintrittswahrscheinlichkeit und Schwere des Risikos in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden sollten. Das Risiko sollte weiters „[...] anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt“.[414]

Um die formalen Anforderungen für den vorliegenden Sachverhalt und Anwendungsfall in ein praktikables methodisches System überzuführen wurde folgendes Modell bzw Template zur Risikobeurteilung entwickelt:

[412] Zudem kann ergänzt werden, welche zusätzlichen Maßnahmen sich bestimmen lassen um die identifizierten Risiken zu mitigieren.
[413] Siehe hierzu insb Art 35 Abs 7 sowie ErwGr 76, 77 und 83 DSGVO; vgl zudem *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 21 sowie *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38 ff.
[414] Vgl ErwGr 76 DSGVO.

Risikobeurteilung (Template)

1) Risikoidentifikation	**Risikobeschreibung**
	Beschreibung und kurze deskriptive Erläuterung des Szenarios, Nennung beteiligter Akteur*innen und Personen,[415] Nennung verarbeiteter Datenkategorien
	Risikoquelle
	Was sind die auslösenden Elemente für den Schadenseintritt? Handelt es sich um eine menschliche oder technische Risikoquelle? **Interne menschliche Quellen:** Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Schaden für die betroffene Person wird entweder billigend in Kauf genommen oder wird von dem*der Verursacher*in beabsichtigt und stellt Ziel der Handlung dar **Externe menschliche Quellen:** Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Angreifer*in oder Verursacher*in außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Systems oder der Betroffenen **Interne / externe technische Quellen:** Systemfehler (Software/Hardware) führen zu Verlust, Veränderung; Nichtverfügbarkeit oder missbräuchlicher Verwendung personenbezogener Daten **Bsp Risikoquelle:** • Interne*r Mitarbeiter*in • Externe*r Mitarbeiter*in • Betroffene • Sonstige *Dritte* • Softwarefehler • Hardwaredefekt (physikalisch) • Umwelteinflüsse (Naturgewalt) • Cyberkriminelle*r (Hacker*in/Schadsoftware) • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) • Geschäftsführung

[415] Siehe hierzu auch die Auflistung an zu prüfenden Organisationen bei *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 30 f.

	Risikoursache
	Was löst den Eintritt des Schadens aus und führt zur „Verwirklichung des Risikos“? Dies dürfte idR in der Nichteinhaltung der Datenschutzgrundsätze (Art 5 Abs 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art 12 bis 22 DSGVO) oder anderer Verstöße gegen die DSGVO (wie zB einen ungerechtfertigte Datentransfers ins Ausland) liegen.[416] **Bsp Ursachen:** • Unbefugte oder unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Für die Betroffenen intransparente Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten • Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten • Verweigerung der Betroffenenrechte • Verwendung der Daten durch die *Verantwortlichen* zu inkompatiblen Zwecken • Verarbeitung nicht vorhergesehener Daten • Verarbeitung nicht richtiger Daten • Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler) • Verarbeitung über die Speicherfrist hinaus • Die Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt (zB weil diese illegitim ist/einer Rechtsgrundlage entbehrt) • Verarbeitung wider dem Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	Welche Schäden und Beeinträchtigungen von Rechten und Freiheiten der Betroffenen lassen sich feststellen? Handelt es sich um einen physischen, materiellen oder immateriellen Schaden?[417] **Bsp physische Schäden:** körperliche Schäden (zB durch falsche medizinische Behandlung), wenn Verstöße gegen die Vertraulichkeit Gewaltverbrechen, einschließlich Stalking, Vorschub leisten; psychologische Schäden (wie zB Angstzustände oder Depressionen) **Bsp materielle Schäden:** wirtschaftliche Schäden, berufliche Nachteile (wie zB entgangene Einstellung oder Beförderung, Jobverlust), Beschneidung staatlicher Leistungen (wie zB Arbeitslosengeld, Sozialhilfe), Diskriminierung (zB bei Versicherungsabschlüssen oder Wohnungssuche), ungerechtfertigte Gebühren oder Bußgelder usw

[416] Siehe hierzu auch *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38 ff.
[417] *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 30 f.

	Bsp immaterielle Schäden: gesellschaftliche und soziale Nachteile (zB Rufschädigung oder Verleumdung, Mobbing, Diskriminierung usw), Schädigung der Privatsphäre (zB das Gefühl, aufgrund von biometrischer Erkennung, oder Tracking über Webseiten, Applikationen und Endgeräte hinweg, ausgespäht zu werden), Einschüchterungseffekte (sog Chilling Effects, wenn Menschen aus Angst davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit auszuleben bzw zu entfalten), ungerechtfertigte Beeinträchtigung von Rechten (durch Verarbeitung ohne ausreichende Rechtsgrundlage)

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Vernachlässigbar (1) - Eingeschränkt (2) - Wesentlich (3) - Maximal (4)	- Vernachlässigbar (1) - Eingeschränkt (2) - Wesentlich (3) - Maximal (4)	- Gering (1-2) - Normal (3-9) - Hoch (12-16)

3) Maßnahmen	**Bestehende Maßnahmen**
	Nennung bestehender technischer, organisatorische und vertraglicher Abhilfemaßnahmen

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Vernachlässigbar (1) - Eingeschränkt (2) - Wesentlich (3) - Maximal (4)	- Vernachlässigbar (1) - Eingeschränkt (2) - Wesentlich (3) - Maximal (4)	- Gering (1-2) - Normal (3-9) - Hoch (12-16)

Der Prozess der datenschutzrechtlichen Risikobeurteilung erfolgt im vorliegenden Fall somit anhand der folgenden vier Teilschritte: Risikoidentifikation, Risikoanalyse und -bewertung, Ermittlung und Bestimmung bestehender Maßnahmen der Risikomitigierung und schließlich die neuerliche Risikoanalyse und -bewertung unter Berücksichtigung der identifizierten Abhilfemaßnahmen. Die zuvor dargelegte Sachverhaltsbeschreibung dient als Informationsgrundlage der Risikobeurteilung.[418] Die Risikoidentifikation bezieht sich auf diese Grundlage und extrahiert daraus für die weitere Risikoanalyse wesentliche datenschutzrechtliche Aspekte wie die Nennung der involvierten Akteur*innen bzw Personen, die Beschreibung der Risikoursache bzw Quelle, sowie die Bestimmung möglicher physischer, materieller oder immaterieller Schäden.

[418] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38 ff.

Die anschließende Risikoanalyse und -bewertung stellt aus methodischer Sicht einen Prozess der Quantifizierung des vorab geschilderten und identifizierten Risikoszenarios dar. Dabei werden Eintrittswahrscheinlichkeit und Schwere des Risikos jeweils anhand der Skalen-Ausprägung „vernachlässigbar", „eingeschränkt", „wesentlich" bzw „maximal" eingestuft.[419] Im Zuge der Risikobeurteilung sind die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu eruieren.[420] Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annahmen zur angemessenen Einstufung des identifizierten Risikoszenarios.[421]

Wert	**Beschreibung**
Vernachlässigbar	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Bedrohung eintreten zu lassen (zB: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
Eingeschränkt	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Bedrohung eintreten zu lassen (zB: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
Wesentlich	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Bedrohung eintreten zu lassen (zB: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
Maximal	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Bedrohung eintreten zu lassen (zB: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit[422]

Wert	**Beschreibung**
Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Eingeschränkt	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Wesentlich	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Tabelle 2: Risikoausprägungen für Schadensausmaß[423]

[419] Die Benennung der Merkmalsausprägung variiert; bei *Martin* et al, Datenschutz-Folgenabschätzung (2020) 47 ist bspw von „geringfügig", „überschaubar", „substantiell" und „groß" die Rede; siehe weiterführend auch *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 31 f; vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 29; vgl *CNIL*, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.

[420] Vgl ErwGr 75 und 76 DSGVO.

[421] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 ff; vgl *CNIL*, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.

[422] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 30 f.

[423] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 f.

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in einer Risikomatrix verortet. Der Risikograd ist methodisch definiert als das Produkt von Eintrittswahrscheinlichkeit und Schadensausmaß.[424] Die Bestimmung des Gesamtrisikos des in Rede stehenden Sachverhalts wäre

$$Risk = \sum_{i=1}^{n} Impact_i \times p_i,$$

wobei **Impact$_i$** für das Schadensausmaß des Risikos **i** und **p$_i$** für dessen Eintrittswahrscheinlichkeit stehen.[425] Auf Basis der Skala von 1 bis 4 (mit den Ausprägungen „vernachlässigbar", „eingeschränkt", „wesentlich" sowie „maximal") ergeben sich Werte von 1 bis 16. Diese werden typischerweise in drei Klassen unterteilt: geringes Risiko, normales Risiko und hohes Risiko.[426] Als Risikoakzeptanzniveau werden Werte < 3 festgelegt, dh alle Risiken mit einem Ergebnis von 1 bis 2 gelten als gering bzw akzeptabel und machen keine weiteren Maßnahmen erforderlich. Hohe Risiken, mit Werten größer als 9, bedürfen hingegen immer einer weiteren Risikobehandlung.[427]

		Eintrittswahrscheinlichkeit			
		Vernachlässigbar	Eingeschränkt	Wesentlich	Maximal
Schadensausmaß	Maximal	Normal (4)	Normal (8)	Hoch (12)	Hoch (16)
	Wesentlich	Normal (3)	Normal (6)	Normal (9)	Hoch (12)
	Eingeschränkt	Gering (2)	Normal (4)	Normal (6)	Normal (8)
	Vernachlässigbar	Gering (1)	Gering (2)	Normal (3)	Normal (4)

Tabelle 3: Risikomatrix

Um der grundrechtlichen Schutzkonzeption des Datenschutzrechts gerecht zu werden, wird im Schrifttum jedoch auch empfohlen, die Beurteilung eines Risikos nicht ausschließlich anhand der quantitativen Matrix von Schadenshöhen (Schwere) und Eintrittswahrscheinlichkeiten zu bestimmen. Vielmehr ist davon auszugehen, dass generell jede Datenverarbeitung einen Eingriff in die Grundrechte der Betroffenen gem Art 7 und 8 der GRC darstellt und sich auch aus einer völlig rechtskonformen Datenverarbeitung bereits ein „normaler" Schutzbedarf ergibt.[428]

[424] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 8 (9).
[425] Siehe kritisch hierzu *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 33.
[426] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 46; vgl hierzu weiterführend auch *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 31.
[427] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 22, 31 ff; vgl auch *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 31 f.
[428] Vgl *Friedewald* et al, Datenschutz-Folgenabschätzung (2017) 31.

Darüber hinaus hat die Folgenabschätzung in einem nächsten Schritt jedenfalls eine Auswahl an Abhilfemaßnahmen, im Sinne von Garantien, Sicherheitsvorkehrungen und Verfahren zur Bewältigung der Risiken und der Sicherstellung des Schutzes personenbezogener Daten, anzuführen.[429] Dabei werden bestehende technische und organisatorische Maßnahmen zur Behandlung und Mitigierung des Risikos ermittelt und aufgezeigt. Die Maßnahmen können die Gestaltung und Entwicklung des Systems ebenso betreffen wie den operativen Betrieb. Im Zuge dessen ist insb den Grundsätzen des Datenschutzes durch Technik (Data Protection by Design) und datenschutzfreundliche Voreinstellungen (Data Protection by Default) Genüge zu tun.[430]

Die in Art 35 Abs 7 lit d DSGVO genannte „Bewältigung" wird gemeinhin auch als „Reduktion" bzw „Eindämmung" verstanden.[431] Über die Maßnahmen zur Mitigerung sollten zumindest alle als „hoch" bewerteten Risiken so weit reduziert werden, dass sie nur noch als „normal" einzustufen sind.[432] Dabei ist es nicht zwangsläufig notwendig, zusätzliche Maßnahmen zu implementieren; mitunter kann es auch sinnvoller sein, bestehende Maßnahmen zu stärken.[433]

In Art 32 Abs 1 DSGVO werden zur Gewährleistung eines angemessenen Schutzniveaus folgende Optionen bzw Maßnahmen der Risikobehandlung angeführt:[434]

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Zusätzlich wird in Art 32 Abs 4 auf Maßnahmen der Zugriffsbeschränkung bzw Zugangskontrollen verwiesen.[435] Die verschiedenen Maßnahmen, Garantien und Verfahren sollen letztlich den Schutz personenbezogener Daten sicherstellen und die Einhaltung der Bestimmungen dieser Verordnung nachweisen.[436]

Nach Ermittlung und Bestimmung der Maßnahmen wird im vorliegenden Modell der Risikobeurteilung der Schritt zur Risikoanalyse und -bewertung wiederholt und eine neuerliche Klassifizierung und

[429] Siehe Art 35 Abs 7 lit d DSGVO; vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 38.
[430] Vgl ErwGr 78 DSGVO.
[431] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 46.
[432] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 47.
[433] Vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 48.
[434] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 33 f.
[435] Für eine Liste typischer Abhilfemaßnahmen siehe die weiterführenden Angaben bei *Martin* et al, Datenschutz-Folgenabschätzung (2020) 48; siehe zudem den Maßnahmenkatalog der CNIL, PIA Manual 2 - Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015, Seite 7 ff; vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 54 ff.
[436] Vgl ErwGr 90 DSGVO.

Errechnung des Risikograds vorgenommen. Über diesen zweiten Analyse- bzw Bewertungsschritt wird der potentielle Einfluss der vorab festgelegten Maßnahmen der Risikomitigierung verdeutlicht.

Abschließend geht es in einer generellen Zusammenschau, um die Feststellung des verbleibenden Restrisikos und der damit Verbundenen weiteren Risikobehandlung durch den *Verantwortlichen*.[437] Dabei kommt vor allem eine weitere Minimierung des Risikos in Frage, indem in der weiteren künftigen Entwicklung des Systems zusätzliche Maßnahmen, die entweder den Schaden oder die Eintrittswahrscheinlichkeit verringern, umgesetzt werden. Zudem kann auch eine gänzliche Eliminierung des Risikos erfolgen, indem die in Rede stehende Datenverarbeitung komplett vermieden wird.[438] Die DSFA mündet damit gem Art 35 Abs 7 lit b DSGVO schließlich in einer Gesamtbewertung der Notwendigkeit und Verhältnismäßigkeit der vorgesehenen Verarbeitungsvorgänge in Bezug auf deren Zweck. Dies beinhaltet auch die Obliegenheit zu prüfen, ob es alternative und datenschutzrechtlich weniger eingreifende Verarbeitungsformen gibt, die ebenfalls eine Zweckerreichung sicherstellen können.[439]

[437] Hierbei ist anzumerken, dass in der IT- und Datensicherheit nicht davon ausgegangen wird, dass absolute Sicherheit erreicht werden kann. Vgl *Jandt* in *Kühling/Buchner* DS-GVO/BDSG (2018) Art 35 Rz 46; siehe weiterführend *Rothmann*, Der Fehler im Feld der Überwachung, in *Winter/Schausberger* (Hrsg) Parapraxis (2016) 65 ff.

[438] Siehe weiterführend jedoch nicht spezifisch datenschutzrechtliche auch *Bundesamt für Sicherheit in der Informationstechnik*, BSI-Standard 100-3 (2008) 17; vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 33 f.

[439] Vgl *Trieb* in *Knyrim*, DatKommArt 35 Rz 112.

5.2 Risikobeurteilung

Auf Basis des vorgestellten methodischen Modells erfolgt in einem nächsten Schritt die eigentliche Umsetzung der Risikobeurteilung. Die Risikobewertung gilt als Kern- bzw Herzstück der DSFA.[440] Dabei ist zu beachten, dass konsequent die Perspektive der Betroffenen eingenommen wird. Der Umfang der DSFA orientiert sich an den vier als Sachverhalt dargelegten Datenverarbeitungsprozessen. Die folgende Liste an Risikobewertungen kann grundsätzlich erweitert und auf andere Szenarien ausgedehnt werden.[441] Darüber hinaus ist die Folgen- und Risikoabschätzung als Prozess zu verstehen und laufend an die tatsächlichen Begebenheiten und Entwicklungen anzupassen und zu aktualisieren.

5.2.1 Unbeabsichtigte Erstellung eines E-ID

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person unterliegt der (irrigen) Annahme, dass sie im Zuge der Beantragung eines Reisepasses oder Personalausweises bei der hierfür zuständigen Passbehörde (Registrierungsbehörde) zwingend eine ID Austria (E-ID) erstellen lassen muss und macht daher von der Opt-out Möglichkeit keinen Gebrauch.
	Risikoquelle
	Interne menschliche Risikoquelle: Behördenmitarbeiter*in der Registrierungsbehörde, welche*r durch unbeabsichtigtes oder beabsichtigtes individuelles Handeln der betroffenen Person signalisiert, dass im Zuge der Beantragung eines Reisepasses oder Personalausweises auch zwingend eine ID Austria (E-ID) erstellt werden muss.
	Risikoursache
	• Unzureichende Informationserteilung • Einschränkung der informationellen Selbstbestimmung • Mangelnde Freiwilligkeit der Einwilligung
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden • Ungewollte Verfügbarkeit personenbezogener Daten • Eröffnung des Potenzials von Identitätsdiebstahl oder -betrug, Datenverlust oder sonstigem Verlust der Vertraulichkeit der Daten, oder einer der anderen nachfolgend beschriebenen Risiken, die mit dem Innehaben eines E-ID einhergehen können, da die betroffene Person hier eigentlich gar keinen E-ID hätte, wenn sich dieses Risiko nicht materialisiert hätte

[440] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 113.
[441] Vgl hierzu auch die Vorgehensweise bei *Bock* et al, Datenschutz-Folgenabschätzung für die Corona-App (2020) 69.

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3) Kommentar: Ein Kommunikationsproblem zwischen Behördenmitarbeiter*in und betroffener Person erscheint möglich.	- Maximal (4) Kommentar: Wenn sich dieses Risiko materialisiert, wird die betroffene Person unfreiwillig dem Potenzial ausgesetzt, dass sich alle folgenden Risiken materialisieren und somit auch das schwerwiegendste der im Folgenden identifizierten Risiken.	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Seitens Behördenmitarbeiter*in erfolgt die Aushändigung einer ID Austria Broschüre, die neben allgemeinen Informationen über die ID Austria auch einen Hinweis auf die Opt-out Möglichkeit beinhaltet. • Darüber hinaus befindet sich ein Hinweis auf die Opt-out Möglichkeit (bzw dessen Bestätigung) auch direkt auf dem Pass- bzw Personalausweisantrag der E-ID-Werber*innen. • Schulung von Behördenmitarbeiter*innen

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.2 Sozialer Druck zur Erstellung bzw Nutzung des E-ID

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass es für Betroffene aufgrund einer weiten Verbreitung des E-ID als Mittel der Authentifizierung im öffentlichen oder privaten Sektor zu Formen sozialen Drucks oder indirekten Zwangs zur Nutzung des E-ID Systems kommt, um bestimmte Services überhaupt in Anspruch nehmen zu können. Das ID Austria System soll zwar grundsätzlich eine deutlich bessere ID Lösung sein als bisherige Ansätze, sowie der E-ID an sich eine Reihe an Vorteilen mit sich bringen kann, defacto kommt es mit der E-ID aber auch zu einer Intensivierung datenschutzrechtlicher Eingriffe. Bei Diensten, die bis dato noch primär analog und anonym genutzt werden, kann es künftig dazu kommen, dass Service Provider die digitale Identifikation mittels staatlich geprüfter Identität verlangen. Dadurch wird die Verarbeitung personenbezogener Daten und der damit einhergehende Grundrechtseingriff zunehmend gefördert. Die betroffenen Personen könnten sich dann zwar bewusst, aber dennoch unfreiwillig für die Erstellung bzw Nutzung der E-ID entscheiden, da sonst bestimmte Verwaltungsprozesse unverhältnismäßig erschwert oder gar nicht mehr möglich wären. Im privaten Bereich wäre beispielhaft das Szenario zu nennen, dass Banken bzw Anbieter*innen von Online-Banking aufgrund von Sicherheitserwägungen nur noch das staatliche Identitätsmanagementsystem für den Login akzeptieren.
	Risikoquelle
	Interne menschliche Quellen: Interne Entscheidungsträger*innen vernachlässigen die Möglichkeit, dass diverse Dienste, Services und Anwendung, die mit dem E-ID System verbunden sind, bzw durch dieses bedient werden, nach wie vor auch analog genutzt und niederschwellig erreicht werden können. **Externe menschliche und strukturelle Quellen:** Größere Zahl von privaten Service Ownern bzw deren Verhalten, das zu entsprechenden Drucksituationen führt. Politische Entscheidungen und/oder die fortschreitende Verwaltungsdigitalisierung könnten zu einem faktischen Zwang zur Verwendung des E-ID führen, weil ohne E-ID bestimmte Verwaltungsprozesse unverhältnismäßig erschwert oder gar nicht mehr möglich sind.
	Risikoursache
	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu entsprechendem Druck zur Nutzung des E-ID Systems. • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer ungewollten bzw unrechtmäßigen Datenverarbeitung. • Einschränkung der informationellen Selbstbestimmung

	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Möglicher Ausschluss von system- oder alltagsrelevanten Diensten, womit auch finanzielle Schäden verbunden sein könnten (zB Unmöglichkeit der Nutzung von Internetbanking führt zu Zusatzkosten) **Immaterielle Schäden:** • Einschränkungen in Teilen der (zB privaten) Lebensführung • Einschränkungen in der Nutzung von Diensten aufgrund der Ablehnung, das ID Austria System zu nutzen • Unfreiwillige Nutzung des ID Austria Systems trotz grundsätzlicher Ablehnung aufgrund von Bedenken • Unfreiwillige oder auch bloß unreflektierte Herausgabe der Identität oder einzelner Attribute, weil diese bei bestimmten Diensten nunmehr verlangt werden bzw deren komfortable Herausgabe ermöglicht wird • Verringerte Anonymität und verstärktes Hinterlassen personenbezogener Datenspuren im Alltagsleben

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Maximal (4)	Wesentlich (3) Kommentar: UU könnten substanzielle Nachteile entstehen; dies sind aber eher Extremfälle.	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Verwaltungsprozesse stehen den Betroffenen nach wie vor auch analog ohne Smartphone zu Verfügung. • Prüfung privater SP bei Akkreditierung/Registrierung insbesondere auf Zweck des Einsatzes des ID Austria Systems und Begründung für anzufordernde Attribute • Spezifizierung der Umstände, unter denen *Dritte* als Unternehmen und Vereine überhaupt teilnehmen können

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Wesentlich (3)	Normal (9)

5.2.3 Staatliche Infrastruktur mit Überwachungspotenzial

1) Risikoidentifikation	**Risikobeschreibung**
	Das E-ID System könnte als technische Basis und Infrastruktur für eine Form von staatlich-zentralisierter Informationssammlung und Datenverarbeitung gesehen werden, die per se Facetten digitaler Überwachung verschiedener gesellschaftlicher Prozesse, Handlungen und Aktivitäten umfasst bzw mit sich bringt. Diese betrifft die Nutzer*innen des E-ID Systems ebenso wie Service Owner bzw Provider. Auch dann, wenn argumentiert wird, dass der aktuelle Zweck des E-ID Systems nicht explizit oder primär in der Überwachung und Kontrolle der Bevölkerung liegt, könnte es künftig zu einer Durchbrechung der Zweckbindung (Function Creep) kommen. Anders als ursprünglich intendiert, könnte das E-ID System dann (im weitesten Sinne) zu Formen der Überwachung der Gesellschaft genutzt werden. Das E-ID System kann diskriminierende Praktiken nach sich ziehen und autoritäre Strukturen zur Disziplinierung der Bevölkerung unterstützen.[442] In der Literatur ist auch von „Policy Windows" in Zeiten gesellschaftspolitischer Krisen die Rede, welche die Ausrollung staatlicher ID-Systeme und deren Nutzung zu Überwachungszwecken begünstigen.[443] Das Risiko betrifft sowohl die österreichische als auch die europäische Gesamtbevölkerung bzw die potentiellen Nutzer*innen des E-ID Systems. Formen der Überwachung und Kontrolle treffen auch private Service Owner bzw Provider. Dabei kommt es zu einer Verarbeitung der E-ID als personenbezogenes Datum an sich, sowie damit verbunden zu einer Verarbeitung diverser staatlich zertifizierte personenbezogener Datenpunkte, Datensätze bzw Register inkl sensibler bzw besonderer Kategorien personenbezogener Daten. So bspw Strafregisterdaten (jedoch lediglich hinsichtlich der Service Provider im Akkreditierungsprozess) oder Fahndungsdaten, jedoch lediglich um festzustellen, ob eine Person eine Registrierung durchführen kann oder ob das Reisedokument als gestohlen registriert ist.
	Risikoquelle
	Interne menschliche Quellen: Unbeabsichtigtes Handeln: Politische Entscheidungsträger*innen implementieren unbedacht ein E-ID System, welches wesentlich aus Datenverarbeitungsprozessen besteht, die eine Form der Überwachung darstellen bzw künftig dafür genutzt werden könnten. Vorsätzliches Handeln: Politische Entscheidungsträger*innen sehen die Risiken potentieller Überwachung, aber nehmen potentielle Schäden für die Betroffenen billigend in Kauf. Zudem kann es zu Missbrauch des E-ID Systems durch einzelne Sachbearbeiter*innen kommen.[444]

[442] Siehe zur Überwachung durch staatliche ID Systeme *Boersma* et al, Histories of State Surveillance in Europe and Beyond (2014) 133 ff, mit historischen Fallbeispielen zu Spanien, Portugal, Belgien und den Niederlanden.
[443] Vgl *Kingdon*; Agendas, Alternatives and Public Policies (1995) in, *Boersma* et al, Histories of State Surveillance in Europe and Beyond (2014) 150 ff.
[444] Vgl *Boersma* et al, Histories of State Surveillance in Europe and Beyond (2014) 133 ff.

	Externe menschliche Quellen: Vorsätzliches Handeln: Staatliche Institutionen und Nachrichtendienste können zum Zweck der Strafverfolgung und Prävention auf das E-ID System zugreifen. **Interne / externe technische Quellen:** Die Architektur des E-ID Gesamtsystems und die damit einhergehende Verarbeitung personenbezogener Daten, stellt per se eine technische Infrastruktur für Praktiken und Prozesse der Überwachung dar. **Risikoquelle:** • Staatliche Institutionen • Interne wie externe Mitarbeiter*innen • Architektur und technische Ausgestaltung des E-ID Systems
	Risikoursache
	• Unbefugte Offenlegung bzw unbefugter Zugriff auf Daten • Verwendung der Daten durch die *Verantwortlichen* zu inkompatiblen Zwecken bzw Verarbeitung gegen den Zweckbindungsgrundsatz • Die Verarbeitung an sich, da das E-ID System per se aus Datenverarbeitungsprozessen besteht, die eine Form von Überwachung und Kontrolle darstellen
	Möglicher Schaden für die betroffenen Personen
	Physische Schäden: Mit Blick auf die historisch belegte (zweckfremde) Nutzung staatlicher ID Systeme, sind sowohl körperliche, materielle wie auch immaterielle Schäden und die Repression spezifischer Bevölkerungsgruppen argumentierbar.[445] **Materielle Schäden:** Form der Diskriminierung, die typischerweise an Überwachungsprozesse anknüpfen, Beschneidung staatlicher Leistungen bzw Ansprüche, Verweigerung des Zutritts zu staatlichen oder privaten Einrichtungen, Verweigerung des Zugriffs auf staatliche oder private Dienste oder Services. **Immaterielle Schäden:** Gesellschaftliche bzw soziale Nachteile durch Beeinträchtigung des politischen Gemeinwesens und der Entfaltungschancen der Einzelnen, Eingriff bzw Verletzung der Privatsphäre (wie etwa das Gefühl oder auch faktisch über biometrische Erkennung oder Tracking ausgespäht zu werden), demokratiepolitische Schäden durch Einschüchterungseffekte (Chilling effects), wenn Betroffene davon absehen, ihre Rechte wahrzunehmen, ihre Persönlichkeit zu entfalten oder ihre Meinung zum Ausdruck zu bringen.

[445] Vgl *Boersma* et al, Histories of State Surveillance in Europe and Beyond (2014) 133 ff.

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Maximal (4)	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Erfüllung der grundlegenden Informationspflichten (Art 13 und 14 DSGVO) • Zusätzliche Informationen über Art, Inhalt und zugrundeliegende informationstechnische Prozesse im Sinne von Transparenz, Vertrauensbildung sowie Checks/Balances durch die interessierte Öffentlichkeit (insb durch Veröffentlichung des DSFA-Berichts) • Durchführung und laufende Adaptierung der DFSA im Hinblick auf technische Änderungen, gesellschaftliche Änderungen, gesetzliche Änderungen • Einbindung der *Datenschutzbeauftragten* • Protokollierung und damit einhergehende Rechenschaft • Möglichkeit der Durchsetzung von Datenschutzrechten (zB Auskunftsersuchen) • SP-Akkreditierung (Zweckbindung, § 18 Abs 2 letzter Satz E-GovG) • VDA weiß nicht, um welche Transaktion es sich handelt. • BRZ ist ISO 27001 zertifiziert (Informationssicherheit)

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.4 Rechtswidriger Zugriff auf Protokolldateien der Anmeldehistorie

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass Transaktionsprotokolle offengelegt bzw zweckwidrig verarbeitet werden und deshalb bekannt wird, an welchen Stellen sich Betroffene angemeldet haben bzw Signaturen durchgeführt wurden. Diese Risikobeurteilung richtet sich an das in der Frontend-Domain betriebene Transaktionsprotokoll (ZLog).
	Risikoquelle
	• Interne*r Mitarbeiter*in • Externe*r Mitarbeiter*in • Sonstige *Dritte* • Softwarefehler • Cyberkriminelle*r (Hacker*in/Schadsoftware), • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) • Geschäftsführung
	Risikoursache
	• Protokolldaten verlassen das ID Austria System oder werden dort zweckwidrig verarbeitet.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Diskriminierung (zB bei Vertragsabschlüssen) • Finanzieller Verlust **Immaterielle Schäden:** • Rufschädigung • Verletzung der Privatsphäre • Wirtschaftliche oder gesellschaftliche Nachteile • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3) Kommentar: Missbräuchlicher Zugriff durch Befugte möglich,	- Maximal (4) Kommentar: Öffentlichwerden des Nutzungsverhaltens kann uU sogar	- Hoch (12)

	ebenso unbefugter Zugriff von außen durch einen Angriff	schlimmer sein als das Öffentlichwerden von Attributsdaten. Man denke zB an Anwendungsfälle des Altersnachweises, mit denen die betroffene Person nicht in Verbindung gebracht werden möchte.	

3) Maßnahmen	**Bestehende Maßnahmen**
	• Mitarbeiter*innen des BRZ werden regemäßig und verpflichtend in den Themen Informationssicherheit und Datenschutz geschult • Es gibt im BRZ diverse Sicherheitsrichtlinien, ua für den Bereich „Informationssicherheit am Arbeitsplatz“. • Weiters werden im ID Austria Umfeld Pentests durchgeführt (letzter Testzeitraum 02/2022). • Das BRZ kann verschiedene Zertifizierungen nachweisen, wie zB ISO 27001, ISO 27018, ISO 22301 sowie ISO 9001. • Die betroffenen Personen werden über die Protokollierung mittels Broschüre, in der App und auf der ID Austria-Website informiert. • Zudem werden künftig zur Absicherung von Transaktions-Logdaten zusätzliche technische und organisatorische Maßnahmen umgesetzt, die über die Standardmaßnahmen, die im BRZ bereits implementiert sind (zB OWASP Top 10), hinausgehen.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Wesentlich (3) Kommentar: Protokollierung der Zugriffe ist auch geeignet, um das Schadensausmaß zu senken, da Missbrauch auffällt und allfällige Korrekturen durchgeführt werden können.	- Normal (6)

5.2.5 Rechtswidriger Zugriff auf Protokolldateien der Identity Provider

1) Risikoidentifikation	**Risikobeschreibung**
	Identity Provider (VDA, eIDAS, SAD, SZRB) validieren Anmeldevorgänge und können Anmeldevorgänge protokollieren. Die Protokollierungsmöglichkeit der Identity Provider ist weniger umfassend als jene der Frontend-Domain, da die Anmeldevorgänge auf mehrere Stellen verteilt werden, und jede Stelle nur die sie erreichenden Anmeldevorgänge protokollieren kann. Dennoch besteht grundsätzlich das Risiko, dass Transaktionsprotokolle einzelner Identity Provider offengelegt bzw zweckwidrig verarbeitet werden und deshalb bekannt wird, an welchen Stellen sich Betroffene angemeldet haben bzw welche Signaturen durchgeführt wurden.
	Risikoquelle
	Externe menschliche Quellen • Interne*r Mitarbeiter*in • Externe*r Mitarbeiter*in • Sonstige *Dritte* • Softwarefehler • Cyberkriminelle*r (Hacker*in/Schadsoftware), • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) • Geschäftsführung
	Risikoursache
	• Unbefugter Zugriff auf Protokolldateien der Identity Provider • Zweckwidrige Verarbeitung der Protokolldateien der Identity Provider
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Diskriminierung (zB bei Vertragsabschlüssen) • Finanzieller Verlust I**mmaterielle Schäden:** • Rufschädigung • Wirtschaftliche oder gesellschaftliche Nachteile • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Maximal (4) Kommentar: Öffentlichwerden des Nutzungsverhaltens kann uU sogar schlimmer sein als das Öffentlichwerden von Attributsdaten. Man denke zB an Anwendungsfälle des Altersnachweises, mit denen man nicht unbedingt in Verbindung gebracht werden möchte.	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Weitgehende Pseudonymisierung der Anmeldedaten vor Übermittlung an Identity Provider. Identity Provider können ohne Zusatzwissen keinen Personenbezug herstellen.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Vernachlässigbar (1)	- Maximal (4)	- Normal (4)

5.2.6 Nichtverfügbarkeit des Systems aufgrund fehlgeschlagener Authentifizierung

1) Risikoidentifikation	**Risikobeschreibung**
	Das System steht den Nutzer*innen nicht zur Verfügung und sie können daher eine Signatur oder eine sonstige Transaktion nicht durchführen. Das kann durch den Ausfall einer essenziellen Systemkomponente verursacht werden; davon unabhängig kann die Ursache auch auf der Ebene der einzelnen Nutzer*innen liegen, die als an sich Berechtigte an der Authentifizierung scheitern (False Negative).[446] Das kann wiederum insbesondere dadurch ausgelöst werden, dass der biometrische Faktor nicht einsatzbereit ist oder nicht korrekt erkannt wird.
	Risikoquelle
	• Endgerät • Interne*r Mitarbeiter*in • Externe*r Mitarbeiter*in • Betroffene • Sonstige *Dritte* • Softwarefehler • Hardwaredefekt (physikalisch) • Umwelteinflüsse (Naturgewalt) • Cyberkriminelle*r (Hacker*in/Schadsoftware)
	Risikoursache
	Das Risiko kann eintreten durch eine Fehlfunktion im Authentifizierungsvorgang, sodass die an sich berechtigte Person es nicht schafft, sich zu authentifizieren (False Negative). Auslöser dafür kann sein, dass der biometrische Faktor nicht einsatzbereit ist oder nicht korrekt erkannt wird. Das kann zB verursacht werden durch: • Fehlfunktion in der Biometriekomponente des Smartphones (dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemhersteller*innen) • Biometriekomponente steht bei einer ganzen Gerätegeneration nicht mehr zur Verfügung, weil sie aufgrund einer dokumentierten Kompromittierung deaktiviert werden musste (dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemhersteller*innen). • Geringfügig geänderte physische Merkmale von Nutzer*innen, durch Verletzungen, Hautprobleme etc Neben dieser spezifischen Ursache kann das Verfügbarkeitsrisiko auch durch viele verschiedene andere Ursachen ausgelöst werden. Zu beachten sind vor

[446] Siehe hierzu weiterführend *Cole*, More than Zero, The Journal of Criminal Law and Criminology (2005) 995 ff (1066 ff).

	allem Systemteile, die vielleicht nicht als kritisch wahrgenommen werden, deren Ausfall aber trotzdem zur Nichtverfügbarkeit des Gesamtsystems führen kann.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Materielle Schäden sind vorstellbar, zB wenn Nutzer*innen rasch eine kostenverursachende Alternative zur ID Austria in Anspruch nehmen müssen, zB durch Zusatzgebühren für manuelle/analoge Prozesse bei Dienstleistungsunternehmen. **Immaterielle Schäden:** • Wirtschaftliche oder gesellschaftliche Nachteile aufgrund mangelnder Datenverfügbarkeit der Signatur oder sonstigen Transaktion

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Wesentlich (3) Kommentar: In manchen Fällen wird ein Ausweichen auf eine handschriftliche Unterschrift leicht möglich sein, in anderen Fällen aber nicht.	- Normal (9)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Unterstützung bzw Dokumentierung (zB FAQ) bzgl Hinterlegung neuer biometrischer Daten am Endgerät • Tlw Nutzung von TAN anstatt Biometrie

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Eingeschränkt (2)	- Normal (4)

5.2.7 Unbefugte Verarbeitung biometrischer Daten

1) Risikoidentifikation	**Risikobeschreibung**
	Auf dem Endgerät der Betroffenen werden zum Zweck der Authentifizierung biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) und somit sensible Daten iSv Art 9 Abs 1 DSGVO verarbeitet. Es besteht das Risiko, dass während der Nutzung der ID Austria verarbeitete biometrische Daten (Fingerabdruck, Face-ID) das Endgerät der Betroffenen verlassen und an *Dritte* gelangen. Die zur Verarbeitung der biometrischen Daten verwendete Software und Hardware steht nicht unter der Kontrolle von ID Austria. Hier verlassen sich sowohl ID Austria als auch die Nutzer*innen darauf, dass Hardware- und Softwarehersteller*innen die Biometriefunktion angemessen absichern, ohne dass diese in der Rolle des *Auftragsverarbeiters* sind. Obwohl dieses Risiko auch ohne ID Austria eintreten kann, kann sich ID Austria diesbezüglich risikoerhöhend auswirken, nämlich dann, wenn die betroffene Person nur deswegen begonnen hat, die Biometriefunktion des Endgeräts zu nutzen, um ID Austria zu nutzen. Für diese Personen bewirkt ID Austria, dass überhaupt erst ein Risiko für ihre biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) entsteht.
	Risikoquelle
	• Sonstige *Dritte* • Softwarefehler • Hardwaredefekt (physikalisch) • Cyberkriminelle*r (Hacker*in/Schadsoftware)
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Finanzieller Verlust **Immaterielle Schäden:** • Identitätsdiebstahl oder -betrug • Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Wesentlich (3) Kommentar: Aufgrund der Unveränderlichkeit der biometrischen Merkmale des Menschen ist ein solcher Schaden idR dauerhaft, dh nicht wiedergutzumachen.	- Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	• Verarbeitung biometrischer Daten auf gesichertem und abgesondertem Modul am Endgerät • Verarbeitung biometrischer Daten erfolgt ausschließlich auf dem Endgerät • Exklusive Einbindung von Endgeräten, welche über entsprechende Sicherheitsmaßnahmen verfügen • Bereitstellung einer alternativen Nutzungsmöglichkeit der ID Austria ohne Biometrie, damit sich Nutzer*innen, welche die Biometriefunktion ihres Endgeräts ansonsten nicht nutzen, diesem Risiko nicht aussetzen müssen; teils ist die Nutzung eines FIDO-Tokens möglich.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Vernachlässigbar (1)	- Wesentlich (3)	- Normal (3)

5.2.8 Gewaltanwendung zur Erlangung des zweiten Faktors

1) Risikoidentifikation	**Risikobeschreibung**
	Es ist nicht ausgeschlossen, dass es im Milieu der schweren Kriminalität auch zu einem Eingriff in die physische Integrität und/oder persönliche Freiheit der Nutzer*innen zur Erlangung des zweiten Faktors kommt. Zu denken ist an körperliche Gewalt oder vergleichbare Handlungen (wie zB Erpressung, Drohung und Einschüchterung), um eine Person beispielsweise zum Scannen ihres Fingerabdrucks (und zur Herausgabe des Passworts) zu zwingen, oder auch an Entführung oder Herbeiführung der Bewusstlosigkeit.
	Risikoquelle
	Externe menschliche Quelle: Vorsätzliches Handeln durch sonstige *Dritte* mit dem Ziel der Schädigung der Betroffenen
	Risikoursache
	Die Ursache liegt in der kriminellen Handlung sowie im Einsatz von Biometrie zur Authentifizierung. In Fällen, in denen die Kriminellen das Passwort ansonsten durch gelindere Maßnahmen (zB Phishing) zu erlangen versucht hätten, kommt es durch den Einsatz von Biometrie tatsächlich zu einer Risikoerhöhung. Zwar kann argumentiert werden, dass jemand auch mit vorgehaltener Waffe zu einer händischen Unterschrift gezwungen werden kann, aber aufgrund der physischen Ungebundenheit der elektronischen Möglichkeiten sind zusätzliche Szenarien und ein anderes Schadensausmaß gegeben, insbesondere da nicht nur an die Signatur, sondern auch an die Login-Möglichkeit auf hohem Vertrauensniveau zu denken ist. Der Beweiswert der elektronischen Signatur ist faktisch höher als jener einer händischen Unterschrift, weil der betroffenen Person das Abstreiten der Authentizität in der Praxis viel schwerer fallen wird. Jede*r kann sich viel leichter vorstellen, dass eine händische Unterschrift gefälscht wurde als eine elektronische Signatur. Bei händischer Unterschrift erscheint es sogar denkbar, dass ein Graphologe nachvollziehen kann, ob der*die Unterschreibende unter Druck steht. Im Fall der elektronischen Signatur ist auch zu bedenken, dass diese im Gegensatz zur physischen Unterschrift neben der Vermutung der Authentizität auch die Vermutung der Integrität impliziert. All diese hier genannten Unterschiede in der (faktischen) Wirkung einer elektronischen Signatur im Vergleich zu einer physischen Unterschrift, könnten Kriminelle zu den oben skizzierten Taten bewegen.
	Möglicher Schaden für die betroffenen Personen
	Physische Schäden: • Verletzung der körperlichen Integrität

	Immaterielle Schäden • Psychologische Schäden

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2) Kommentar: In seltenen Einzelfällen denkbar; soweit bekannt gibt es bisher keine derartigen Fälle in Österreich trotz weiter Verbreitung biometrischer Mechanismen bei Smartphones	- Maximal (4) Kommentar: Gefahr dauerhafter körperlicher oder psychischer Schäden	- Normal (8)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Abschreckende Wirkung des Strafrechts

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.9 Identitätsdiebstahl durch Kompromittierung der biometrischen Absicherung

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass ein biometrischer Mechanismus des Smartphone-Betriebssystems, der von ID Austria genützt wird, kompromittiert oder umgangen wird.[447] Erhöht wird dieses Risiko durch zahlreiche veraltete Gerätegenerationen, die noch in Betrieb sind, aber keine Sicherheitsupdates mehr erhalten sowie die verzögerte Verfügbarkeit von Updates auch bei aktuellen Geräten vieler Hersteller*innen. Bereits in der Vergangenheit wurden immer wieder die Biometriesysteme von Smartphones gehackt.[448] Es ist jedoch nicht gesichert, dass ein solcher erfolgreicher Angriff auch künftig im Sinne der Responsible Disclosure den Hersteller*innen kommuniziert und in weiterer Folge veröffentlicht wird; auch aktuelle Systeme könnten bereits kompromittiert sein, ohne dass dies der Öffentlichkeit bekannt ist. Wird eine solche Kompromittierung öffentlich bekannt, könnten die Hersteller*innen gezwungen sein, die kompromittierte Biometriefunktionalität zu deaktivieren und es tritt anstatt des hier beschriebenen Risikos das (separat beschriebene) Risiko der Nichtverfügbarkeit ein.
	Risikoquelle
	Externe menschliche Quellen: Vorsätzliches Handeln: Ein*e Angreifer*in versucht bewusst auf diese Weise den E-ID bzw die Identität der betroffenen Person zu übernehmen.
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Mangelnde Kontrolle über die Systeme der Smartphone- und Betriebssystem-Hersteller*innen • Strukturelle Probleme der Biometrie • Veraltete Gerätegenerationen: Viele Android- und Apple-Geräte, die im Umlauf sind, erhalten keine Sicherheitsupdates mehr, funktionieren aber noch einwandfrei und werden daher weiterverwendet; das Bewusstsein für diese Problematik ist bei vielen Nutzer*innen gering. • Mangelnde Absicherung des Smartphones bzw leichtfertiges aus der Hand geben (zB unbeaufsichtigt lassen, zur Handy Reparatur geben, etc)
	Möglicher Schaden für die betroffenen Personen
	Die Angreifer*innen sind in der Lage, sich elektronisch als die betroffene Person auszugeben und für diese wirksame Erklärungen abzugeben, mit potenziell weitreichenden Folgen.

[447] Siehe bspw https://www.derstandard.at/story/2000131930683/augenlid-schlafender-freundin-geoeffnet-um-app-zu-entsperren-mann-stahl (abgerufen am 22. 04. 2022).
[448] https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid (abgerufen am 22. 04. 2022).

	Materielle Schäden: • Finanzieller Verlust (zB Durchführung einer Überweisung) • Wirtschaftliche Nachteile (zB Abschluss eines Vertrages, Schenkung) **Immaterielle Schäden:** • Gesellschaftliche und soziale Nachteile (wie etwa Rufschädigung) durch Zugriff auf sensible Anwendungen (insb ELGA) • Ungerechtfertigte Beeinträchtigung von Rechten • Dauerhafter Verlust subjektiv besonders wertvoller Rechtspositionen durch Zugriff auf hoheitliche Anwendungen (insb FinanzOnline) • Erschwerend kommt hinzu, dass im Fall einer Kompromittierung die Biometriefunktion nicht einfach durch ein anderes biometrisches Element ersetzt werden kann, wie dies zB bei einem Passwort möglich ist, indem man ein kompromittiertes Passwort durch ein neues ersetzt.

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	-Wesentlich (3)	-Maximal (4) Kommentar: Durch Identitätsdiebstahl und/oder Abschluss von Rechtsgeschäften im Namen der betroffenen Person, können auch unumkehrbare Konsequenzen eintreten, die nicht überwunden werden können.	- Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Teils ausweichen auf FIDO-Token möglich • A-Trust betreibt einen Prozess, der bestimmte Geräteklassen sofort vom System ausschließen kann, wenn zB gravierende Probleme bei Secure Enclaves/Biometrie bekannt werden. • Root Checks • Key/App-Attestation-Verfahren (teilweise aktiv) • Niederschwellige Zurücksetzungsmöglichkeit des Endgerätes

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.10 Identitätsdiebstahl durch Unterschieben eines biometrischen Merkmals

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass im Zuge des Registrierungsprozesses/Ausstellungsprozesses beim erstmaligen Binden der biometrischen Faktoren an den E-ID der betroffenen Person ein*e Angreifer*in es schafft, stattdessen die eigenen biometrischen Faktoren an den E-ID der betroffenen Person zu binden und somit die Verfügungsgewalt über den E-ID der betroffenen Person erlangt.
	Risikoquelle
	Interne menschliche und strukturelle Risikoquelle: Unbeabsichtigtes Handeln: Der Eintritt dieses Risikos kann dadurch begünstigt werden, dass sich die betroffene Person nicht bewusst ist, dass für die eigene Person ein E-ID ausgestellt wird oder wie diese Ausstellung abläuft. **Externe menschliche Quellen:** Vorsätzliches Handeln: Ein*e Angreifer*in versucht bewusst auf diese Weise im Zuge der Registrierung, wenn der biometrische Faktor noch nicht als Absicherung wirkt, sondern gerade neu angelegt wird, den E-ID zu “kapern”. Die Möglichkeiten dafür können reichen bis hin zum Anbieten einer falschen ID Austria-App im App Store.
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Unwissen der betroffenen Person • Wenig erprobte Prozesse und wenig erfahrenes Personal in der Anfangsphase (bei möglicherweise gleichzeitig hoher Fallzahl)
	Möglicher Schaden für die betroffenen Personen
	Der*die Angreifer*in ist in der Lage, sich elektronisch als die betroffene Person auszugeben und für diese wirksame Erklärungen abzugeben, mit potenziell weitreichenden Folgen. **Materielle Schäden:** • Finanzieller Verlust • Wirtschaftliche Nachteile **Immaterielle Schäden:** • Gesellschaftliche und soziale Nachteile (wie etwa Rufschädigung) • Ungerechtfertigte Beeinträchtigung von Rechten • Dauerhafter Verlust subjektiv besonders wertvoller Rechtspositionen

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Maximal (4) Kommentar: Durch Identitätsdiebstahl und/oder Abschluss von Rechtsgeschäften im Namen der betroffenen Person können auch unumkehrbare Konsequenzen eintreten, die nicht überwunden werden können.	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Registrierung erfordert ein aktives Zu-Tun der betroffenen Person • Erfordernis eines persönlichen Erscheinens bei der Behörde • Vorlage von amtlichem Lichtbildausweis und Prüfung durch die Behörde • Prüfung des vorgelegten Lichtbilds auf Übereinstimmung mit der anwesenden Person • SMS, App und Vorregistrierung: Verfügungsgewalt über Mobiltelefon erforderlich • Schulung der Behörden, dass Registrierung nur persönlich erfolgen darf • Allfällige strafrechtliche Relevanz des Verhaltens

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.11 Identitätsdiebstahl durch mangelnde Sicherheit der Anmeldung

1) Risikoidentifikation	**Risikobeschreibung**
	Das System umfasst verschiedene Anmeldevarianten (zB Anmeldung über einen Browser oder eine Third-Party-App). Soweit einzelne Anmeldevarianten niedrigeren Sicherheitsvorkehrungen unterliegen als andere (etwa Authentifizierung nur mit Telefonnummer und Passwort), ist es unbefugten *Dritten* erleichtert einen Anmeldevorgang auszulösen bzw ohne Wissen des *E-ID-Inhabers* die Funktion der Signaturerstellung für den Abschluss von diversen Verträgen zu missbrauchen.
	Risikoquelle
	Externe menschliche Risikoquelle: • Sonstige *Dritte* • Cyberkriminelle*r (Hacker*in/Schadsoftware), • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung)
	Risikoursache
	Unbefugte Auslösung eines Anmeldevorgangs aufgrund des verringerten Sicherheitsniveaus einer Anmeldevariante, indem diese mehrere Authentifizierungsfaktoren als zweiten Faktor zulässt.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Finanzieller Verlust • Wirtschaftliche Schäden **Immaterielle Schäden:** • Gesellschaftliche und soziale Nachteile (zB Rufschädigung) • Schädigung der Privatsphäre • Ungerechtfertigte Beeinträchtigung von Rechten • Dauerhafter Verlust subjektiv besonders wertvoller Rechtspositionen

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3) Kommentar: Es ist denkbar, dass ein Service Provider ausschließlich Anmeldevarianten anbietet, welche einen zweiten Faktor verlangen. Soweit das nicht zutrifft, kann ein*e	- Wesentlich (4) Kommentar: Anschein der Rechtmäßigkeit im Rechtsverkehr	- Hoch (12)

	Angreifer*in verschiedene Anmeldevarianten ausprobieren.		

3) Maßnahmen	**Bestehende Maßnahmen**
	• Erfordernis eines zweiten Faktors in allen Anmeldevarianten • Möglichkeit zur Einsicht in Transaktions-Logdaten durch Betroffene, um Anmeldevorgänge nachvollziehen zu können

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Wesentlich (4)	- Normal (8)

5.2.12 Identitätsdiebstahl durch strukturelle Schwächen des Konzepts Passwort

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass ein*e Angreifer*in das Passwort der betroffenen Person erlangt und in weiterer Folge die Verfügungsgewalt über deren E-ID erlangt. Das kann durch sog Phishing erfolgen, durch Erraten oder auf andere Weise. Das Konzept Passwort, wenn auch enorm weit verbreitet und etabliert, weist aus der Perspektive der Informationssicherheit weitreichende Schwächen auf. Diese reichen von der Problematik, dass Betroffene zu einfache, zu kurze und damit erratbare Passwörter festlegen und diese mehrfach verwenden, bis hin zu der Anfälligkeit für Phishing-Attacken, also das gezielte Abfragen des Passworts durch eine*n Angreifer*in unter Vorspiegelung falscher Tatsachen, wie insbesondere einer gefälschten Eingabemaske.
	Risikoquelle
	Interne menschliche und strukturelle Risikoquelle: Menschliche Schwächen aufseiten der betroffenen Person sind eine wesentliche Ursache der strukturellen Schwächen des Konzepts Passwort. Passwörter werden häufig zu kurz und zu einfach gewählt, werden mehrfach verwendet, es wird sorglos damit umgegangen und auch das Phishing nützt letztlich die Leichtgläubigkeit und Unerfahrenheit von Betroffenen aus. Mit diesen psychologischen Faktoren muss deshalb gerade in einem so breit ausgerollten System gerechnet werden. **Externe menschliche Quellen:** Vorsätzliches Handeln: Ein*e Angreifer*in nützt die beschriebenen menschlichen und strukturellen Schwächen aus, um das Passwort zu erraten oder zu erlangen. Die Möglichkeiten dafür können reichen bis hin zum Anbieten einer falschen ID Austria-App im App Store.
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Leichtgläubigkeit der betroffenen Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit Passwörtern
	Möglicher Schaden für die betroffenen Personen
	Der*die Angreifer*in ist in der Lage, sich elektronisch als die betroffene Person auszugeben und für diese wirksame Erklärungen abzugeben, mit potenziell weitreichenden Folgen. **Materielle Schäden:** • Finanzieller Verlust • Wirtschaftliche Nachteile **Immaterielle Schäden**

	• Gesellschaftliche und soziale Nachteile (wie etwa Rufschädigung) • Ungerechtfertigte Beeinträchtigung von Rechten • Dauerhafter Verlust subjektiv besonders wertvoller Rechtspositionen

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Maximal (4) Kommentar: Durch Offenlegung personenbezogener Daten können auch unumkehrbare Konsequenzen eintreten, die nicht überwunden werden können.	- Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Im Fall der erstmaligen Authentifizierung sind die Faktoren Wissen, Besitz und Eigenschaft erforderlich. • Passwort benötigt eine Minimallänge von mindestens 8 Zeichen. • Ab einer gewissen Anzahl an Fehleingaben erfolgt Sperrung durch VDA.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Vernachlässigbar (1)	- Maximal (4)	- Normal (4)

5.2.13 Mangelhafte Akkreditierung behördlicher Service Owner bzw Provider

1) Risikoidentifikation	**Risikobeschreibung**
	Aufgrund einer mangelhaften Prüfung bzw Akkreditierung der behördlichen Service Provider kann es zu einer unberechtigten Verarbeitung personenbezogener Daten bzw einem unberechtigten Einsatz des E-ID kommen. Dadurch werden (Identitäts-)Daten sowie diverse weitere Attribute von Betroffenen an Behörden übermittelt, die eigentlich nicht berechtigt sein sollten, diese Daten entgegenzunehmen. Das Risiko entsteht durch eine fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements für Service Owner bzw Provider. Im Hinblick auf das Legalitätsprinzip ist das Handeln der behördlichen Provider auf eine entsprechende Rechtsgrundlage zu stützen. Diese sollte verpflichtend geprüft und nachgewiesen werden. Die Verarbeitung der personenbezogenen Daten der Betroffenen hat einer strengen Zweckbindung zu folgen. Wesentliche Akteur*innen in diesem Szenario sind behördliche Service Provider, die verantwortlichen Betreibenden des E-ID Systems sowie betroffene Personen, die das E-ID System nutzen.
	Risikoquelle
	Interne*r Mitarbeiter*in bzw strukturelle und organisatorische Mängel in der Qualität der Registrierung und Akkreditierung der Provider. Der potentielle Schaden für die Betroffenen wird billigend in Kauf genommen.
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Unbefugte Offenlegung von und Zugang zu Daten • Verwendung der Daten durch die *Verantwortlichen* zu inkompatiblen Zwecken • Verarbeitung wider dem Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: • Wirtschaftliche oder gesellschaftliche Nachteile • Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Eingeschränkt (2)	- Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	• Nachträgliche stichprobenartige Überprüfung

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Vernachlässigbar (1)	- Eingeschränkt (2)	- Gering (2)

5.2.14 Zweckwidrige Verarbeitung durch Service Owner

1) Risikoidentifikation	**Risikobeschreibung**
	Attribute sind nach ihrer Auslieferung an den Service Owner dem Verfügungsbereich des E-ID Systems entzogen. Es besteht das Risiko, dass Service Owner eine gesetzeswidrige (insb nicht im Einklang mit der DSGVO stehende) Datenverarbeitung der Attribute durchführen. Zudem eröffnet die Datenhaltung durch Service Owner auch erweiterte Angriffsvektoren für *Dritte*.
	Risikoquelle
	Externe menschliche Quellen: • Entscheidungsträger*innen / Beschäftigte der Service Owner • Cyberkriminelle*r (Hacker*in/Schadsoftware), • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) • Sonstige *Dritte*
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Für die Betroffenen intransparente Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten • Verarbeitung über die Speicherfrist hinaus • Verarbeitung wider dem Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Zugriff auf und Verarbeitung von personenbezogenen Daten zum wirtschaftlichen oder beruflichen Nachteil der Betroffenen • Diskriminierung durch gezieltes Auslesen spezifischer personenbezogener Daten und deren schädliche Verwendung gegen die Betroffenen • Denkbar ist im Einzelfall auch eine Ausforschung spezifischer Personen, um diesen physisch zu schaden. **Immaterielle Schäden:** • Gesellschaftliche und soziale Nachteile (zB Rufschädigung oder Verleumdung, Mobbing, Diskriminierung usw) • Schädigung der Privatsphäre, Einschüchterungseffekte • Ungerechtfertigte Beeinträchtigung von Rechten (durch Verarbeitung ohne ausreichende Rechtsgrundlage) • Verhinderung der Kontrolle durch betroffene Personen • Beeinträchtigung der informationellen Selbstbestimmung

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Maximal (4) Kommentar: Verschiedene Optionen für Missbrauch stehen offen.	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Bestätigung der Einhaltung gesetzlicher Bestimmungen durch den Service Owner • Besonderer Hinweis auf Einhaltung der DSGVO • Besonderer Hinweis auf Grundsatz der Zweckbindung • Möglichkeit des Ausschlusses aus dem E-ID

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Maximal (4)	- Normal (8)

5.2.15 Zweckwidrige Zusammenführung von Attributen

1) Risikoidentifikation	**Risikobeschreibung**
	Ein Service Owner (SO) als *Verantwortlicher* im privaten Bereich kann mehrere Service Provider (SP) bzw Anwendungen registrieren und akkreditieren lassen und daher verschiedene Anwendungen anbieten. SO können als *Verantwortliche* im privaten Bereich mehrere SP, welche verschiedene Attribute abfragen, registrieren. Das bereichsspezifische Kennzeichen wird für jeden SO (konkret aus dessen Stammzahl) errechnet. Registriert ein SO mehrere SP, werden Attribute an alle registrierten SP unter dem gleichen bereichsspezifischen Kennzeichen (der SO) ausgeliefert. Dadurch besteht das Risiko einer Vermengung der eigentlich zu verschiedenen Zwecken erhobenen Attribute.
	Risikoquelle
	Externe menschliche Quellen: • Entscheidungsträger*innen / Beschäftigte der Service Provider
	Risikoursache
	Verarbeitung wider dem Zweckbindungsgrundsatz (bezogen auf den im Zuge der Registrierung eines Service Providers angegebenen Zweck)
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: • Ungerechtfertigte Beeinträchtigung von Rechten durch Verarbeitung ohne ausreichende Rechtsgrundlage (zweckbezogene Einwilligung) • Bildung eines Profils (Erfassung von Daten aus verschiedenen Lebensbereichen) • Beeinträchtigung der informationellen Selbstbestimmung

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3) Kommentar: Eine Trennung nach Attributszwecken der verschiedenen Service Provider ist möglich, wird durch das System aber nicht befördert bzw erzwungen.	- Eingeschränkt (2) Kommentar: Das System bietet eine beschränkte Anzahl an Attributen an.	- Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	• Bestätigung der Einhaltung gesetzlicher Bestimmungen durch den Service Owner • Besonderer Hinweis auf Einhaltung der DSGVO • Besonderer Hinweis auf Grundsatz der Zweckbindung • Möglichkeit des Ausschlusses aus dem E-ID

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Eingeschränkt (2)	- Eingeschränkt (2)	- Normal (4)

5.2.16 Rechtswidrige Verarbeitung durch die systembetreibenden Verantwortlichen

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass es im Rahmen der komplexen Verbindung der verschiedenen Systembetreibenden (insb zwischen BMDW, BMI, Passbehörden, Meldebehörden) zu einer Missachtung der Zweckbindung kommt oder eine rechtswidrige Verarbeitung daraus resultiert, dass einzelne der (Gemeinsam-) *Verantwortlichen* die Grenzen ihrer gesetzlichen Aufgabenerfüllung überschreiten
	Risikoquelle
	Interne menschliche Risikoquellen: Bei *Verantwortlichen* tätige Personen, die Daten entgegen der vorgesehenen Weise zweckwidrig bzw überschießend verarbeiten **Interne technische Risikoquellen:** Architektur/Design lässt Zugriff auf mehr Daten zu, als dies unbedingt zur Zweckerreichung nötig ist.
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Für die Betroffenen intransparente Verarbeitung, weil dahinter liegende Prozesse komplex und schwer einsehbar sind • Unbefugte Offenlegung von und Zugang zu Daten, zB durch einen *Verantwortlichen* an anderen beteiligten *Verantwortlichen*, dem Zugang nicht zustünde • Verwendung der Daten durch die *Verantwortlichen* zu inkompatiblen Zwecken/Verarbeitung wider dem Zweckbindungsgrundsatz (etwa zur Ausforschung von Personen)
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Zugriff auf und Verarbeitung von personenbezogenen Daten zum wirtschaftlichen oder beruflichen Nachteil der Betroffenen • Diskriminierung durch gezieltes Auslesen spezifischer personenbezogener Daten und deren schädliche Verwendung gegen die Betroffenen • Denkbar ist im Einzelfall auch eine Ausforschung spezifischer Personen, um diesen physisch zu schaden. **Immaterielle Schäden:** • Für die Betroffenen kann es zu sozialen wie gesellschaftlichen Nachteilen wie Rufschädigung, Verleumdung oder Diskriminierung kommen. • Durch den rechtswidrigen Zugriff auf die Daten kann es zu einer Verletzung der Privatsphäre der Betroffenen und Formen der Überwachung kommen.

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Maximal (4) Kommentar: Sofern keine Maßnahmen vorliegen, ist in einem derart komplexen Gesamtsystem mit an Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass einzelne Verarbeitungsvorgänge überschießend vorgenommen werden.	- Wesentlich (3) Kommentar: Der rechtswidrige Zugriff und die zweckwidrige Verarbeitung können für die Betroffenen zu wesentlichen Schäden führen.	- Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen • Schulungen von Mitarbeiter*innen im Hinblick auf Umgang mit personenbezogenen Daten • Klare Kommunikation und Aufklärung über Konsequenzen • Kontrolle von Zugriffen interner Mitarbeiter*innen auf Daten • Technische Ausgestaltung iSd Minimierung von Zugriffsmöglichkeiten (zB unverschlüsselte Stammzahl nur SZR zugänglich)

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	- Wesentlich (3)	- Wesentlich (3)	- Normal (9)

5.2.17 Intransparenz der Datenverarbeitung im Rahmen des E-ID Systems

1) Risikoidentifikation	**Risikobeschreibung**
	Ein weiteres Risiko könnte sein, dass das datenschutzrechtliche Prinzip der Transparenz nicht gewährleistet werden kann. Es käme für die Betroffenen zu einer nicht nachvollziehbaren, unklaren Datenverarbeitung. Die Einwilligung in die Verarbeitung würde nicht in informierter Weise bzw in Kenntnis der Sachlage erfolgen. Der *Verantwortliche* kommt den Informationspflichten zwar nach, die Betroffenen könnten aufgrund der technischen und funktionalen Komplexität des E-ID Systems jedoch nicht in der Lage sein, die Auswirkungen des Systems auf ihre Rechte und Freiheiten entsprechend zu beurteilen. Dies kann dazu beitragen, dass die adressierte Bevölkerung kein Vertrauen in das System hat und die ID Austria nicht genutzt wird. Das Risiko betrifft zunächst die Benutzer*innen des E-ID Systems, wenn diese nicht in angemessener Weise einschätzen können, in welcher Weise ihre personenbezogenen Daten von wem weiterverarbeitet werden. Das Risiko betrifft auch die verantwortlichen Betreibenden sowie behördliche und private Service Provider, wenn es um die Frage der Rechtsgrundlage zur Datenverarbeitung geht. Dabei geht es insb um die Verarbeitung von Attributen in Verbindung mit Anwendungen der Service Provider. Dies kann über entsprechende Register auch die Verarbeitung sog besonderer Kategorien personenbezogener Daten umfassen. Zudem werden im Rahmen des E-ID Systems biometrische Merkmale (jedoch ausschließlich lokal auf den Geräten der jeweiligen Benutzer*innen) sowie Daten aus Straf- sowie Fahndungsregistern (jedoch ausschließlich in den Registrierungsprozessen) verarbeitet.
	Risikoquelle
	Interne menschliche Risikoquelle: Es handelt sich um Unzulänglichkeiten in der Bereitstellung von Informationen zur Erfüllung der Informationspflicht. Die Betroffenen scheitern im Verständnis der technischen Komplexität des E-ID Systems; Risikoquelle sind in diesem Sinne unzureichend beschriebene Datenschutzinformationen. Der Schaden für die Betroffenen wird üblicherweise billigend in Kauf genommen.
	Risikoursache
	• Unzureichende Informationen bzw intransparente Verarbeitung • Unbefugte bzw unrechtmäßige Durchführung der Verarbeitung selbst, weil diese illegitim ist bzw der Erfüllung der formalen Anforderungen einer Einwilligung als Rechtsgrundlage entbehrt
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: • Schädigung der Privatsphäre (wie etwa das Gefühl, aufgrund von biometrischer Erkennung oder Tracking über Webseiten, Applikationen und Endgeräte hinweg, ausgespäht zu werden);

	• Einschüchterungseffekte (sog Cilling Effects, wenn Menschen aus Angst davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit auszuleben bzw zu entfalten) • Ungerechtfertigte Beeinträchtigung von Rechten (durch Verarbeitung ohne ausreichende Rechtsgrundlage)

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Maximal (4)	- Wesentlich (3)	- Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Es wird eine Datenschutzerklärung in einfacher und klarer Sprache bereitgestellt.[449] • Es werden FAQs zu Sicherheit und Datenschutz bereitgestellt.[450] • Das ID Austria System wird über die Website „oestrreich.gv.at“ via FAQs sowie durch veröffentlichte Whitepapers und Präsentationsunterlagen grundlegend erklärt.[451] • Es wird eine Datenschutz-Folgenabschätzung durchgeführt und der interessierten Öffentlichkeit zu Verfügung gestellt.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Wesentlich (3)	- Normal (9)

[449] Siehe https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 22. 04. 2022).
[450] Siehe https://www.oesterreich.gv.at/themen/dokumente_und_recht/id-austria/haeufige-fragen.html sowie https://eid.egiz.gv.at/infos/technische-whitepaper/ (abgerufen am 22. 04. 2022).
[451] Siehe https://www.oesterreich.gv.at/id-austria.html (abgerufen am 22. 04. 2022).

5.2.18 Unbewusste oder irrtümliche Datenherausgabe

1) Risikoidentifikation	**Risikobeschreibung**
	Es besteht das Risiko, dass eine betroffene Person bestimmte Daten über das E-ID System an einen *Dritten* herausgibt, ohne dass ihm das (zur Gänze) bewusst ist. Mit dem E-ID System wird erstmals eine Möglichkeit eröffnet, hoheitlich qualifizierte personenbezogene Daten niederschwellig digital an *Dritte*, insbesondere Private, weiterzugeben. Es besteht die Gefahr, dass den Nutzer*innen aufgrund der Einfachheit dieser Prozesse die Tragweite ihrer Handlungen nicht bewusst wird. Das kann irrtümlich erfolgen oder von den Daten empfangenden *Dritten* sogar bewusst herbeigeführt werden, denn diese haben einen Anreiz, an die über das E-ID System bereitgestellten hochqualitativen Daten heranzukommen.
	Risikoquelle
	Interne menschliche und strukturelle Risikoquelle: Unbeabsichtigtes Handeln: Besonders Menschen, die im Umgang mit digitalen Diensten nicht besonders geübt oder körperlich eingeschränkt sind, können rasch Vorgänge auslösen, die ihnen nicht bewusst sind und die sie eigentlich nicht auslösen wollten. Dieses Risiko besteht jedoch auch im Fall herkömmlicher Nutzer*innen. Zudem ist empirisch erwiesen, dass datenschutzrechtliche Informationstexte idR kaum gelesen werden, sondern die Betroffenen einfach auf „Weiter“ klicken, um möglichst rasch ans Ziel zu gelangen.[452] **Externe menschliche Quellen:** Vorsätzliches Handeln: *Dritte*, die Daten erlangen wollen, haben einen Anreiz, die oben beschriebenen Irrtümer, Passivität oder Ignoranz herbeizuführen, um den Betroffenen ihre Daten zu entlocken.
	Risikoursache
	• Unaufmerksamkeit der betroffenen Person • Unwissen der betroffenen Person • Körperliche Einschränkungen der betroffenen Person (zB Sehschwäche, motorische Einschränkungen in Bezug auf die Touch-Bedienung) • Leseschwäche der betroffenen Person • Ignoranz/Ungeduld der betroffenen Person • Intransparente Verarbeitung • Bewusste Herbeiführung des Irrtums/der unbewussten Handlung • Unübersichtliches grafisches Userinterface (GUI) bzw mangelhafte Usability der in Rede stehenden Applikation

[452] Siehe hierzu weiterführend *Solove*, The Myth of the Privacy Paradox, George Washington Law Review (2020); *McDonald/Cranor*, The Cost of Reading Privacy Policies, in: Journal of Law and Policy for the Information Society, (2008) Vol 4, No. 3, 543-568; *Rothmann*/*Buchner*, Der typische Facebook-Nutzer zwischen Recht und Realität, in: DuD (2018) Volume 42 (6), 342-346.

	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: wirtschaftliche Schäden, berufliche Nachteile (zB entgangene Einstellung oder Beförderung, Jobverlust), Beschneidung staatlicher Leistungen (zB Arbeitslosengeld, Sozialhilfe), Diskriminierung (zB bei Versicherungsabschlüssen oder Wohnungssuche), ungerechtfertigte Gebühren usw **Immaterielle Schäden:** gesellschaftliche und soziale Nachteile (zB Rufschädigung oder Verleumdung, Mobbing, Diskriminierung usw), Schädigung der Privatsphäre (zB das Gefühl ausgespäht zu werden), ungerechtfertigte Beeinträchtigung von Rechten (durch Verarbeitung ohne ausreichende Rechtsgrundlage), Misstrauen in das System, Hemmungen, das E-ID System weiter zu nutzen

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Maximal (4) Kommentar: Durch Offenlegung personenbezogener Daten können auch unumkehrbare Konsequenzen eintreten	- Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Niederschwellige Erreichbarkeit der Datenschutzerklärungen der Service Provider vor Anmeldung • Transparente, leicht erreichbare Informationserteilung durch *Verantwortlichen* • Stringente FAQs zu den wichtigsten Funktionen des E-ID

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Maximal (4) Kommentar: Die Maßnahmen beeinflussen ihrer Natur nach nur die Eintrittswahrscheinlichkeit, nicht jedoch das Schadensausmaß.	- Normal (8)

5.2.19 Abhängigkeit in der Nutzung der Ökosysteme von Google und Apple

1) Risikoidentifikation	**Risikobeschreibung**
	Für die Zugänglichmachung sowie die weitere Verwendung der staatlichen App „Digitales Amt“ wird die technische Infrastruktur US-amerikanischer IT-Konzerne genutzt. Die verantwortlichen Betreibenden des E-ID Systems in Form der österreichischen Ministerien begeben sich damit in ein technisches Abhängigkeitsverhältnis mit transatlantischen Diensten. Dies kann sich einerseits auf die Verfügbarkeit des Systems auswirken und dazu führen, dass diese aufgrund rechtspolitischer Entwicklungen nicht mehr wie geplant gegeben ist. Darüber hinaus werden die Betroffenen damit einmal mehr dazu angehalten, sich entsprechende Konten/Accounts bei den transatlantischen Unternehmen anzulegen bzw mit diesen zu kontrahieren. Über die Nutzung der Technologie bzw der Betriebs- und Ökosysteme (App Stores) von Google und Apple kann es weiters zu einer Datenverarbeitung zu inkompatiblen Zwecken kommen. Es besteht dann bspw das Risiko, dass die dabei (aus vertragsrechtlichen oder technischen Gründen) anfallenden Daten zu Werbezwecken weiterverarbeitet werden, da eine derartige Verwendung personenbezogener Daten als ein zentraler Bestandteil der Geschäftsmodelle dieser Unternehmen gilt. Im Zuge dessen kommt es zudem zu einem transatlantischen Datentransfer und dem damit verbundenen Risiko des Zugriffs auf die Daten durch US-Sicherheitsbehörden. Betroffen sind in erster Linie die Nutzer*innen der App, deren Bezug über die Ökosysteme von Google und Apple erfolgt.
	Risikoquelle
	Interne menschliche und strukturelle Quelle: Management-Entscheidung auf Seiten der verantwortlichen Betreibenden des E-ID Systems, zur Nutzung der Infrastruktur von Google und Apple als Plattformprovider für die Distribution der App „Digitales Amt“. Man sieht sich aus Sicht der Betreibenden dazu gezwungen, auf die Plattformen und Technologien *Dritter* zurückzugreifen, um das E-ID System zu implementieren und für weite Teile der Bevölkerung möglichst einfach verfügbar zu machen bzw die Nutzung zu fördern. Vorsätzliches Handeln: Schaden für die Betroffenen wird billigend in Kauf genommen, weil bspw versucht wird die niederschwellige Zugänglichkeit und Benutzer*innenfreundlichkeit der ID Austria zu erhöhen.
	Risikoursache
	• Verarbeitung wider Treu und Glauben durch die Verflechtung einer staatlichen E-Government-Anwendung mit börsennotierten US-amerikanischen IT-Konzernen, da keine eigene Distributionsplattform ohne Weiterverarbeitung der Nutzer*innendaten zu Werbezwecken verwendet wird • Datenverarbeitung wird nicht auf das notwendige Maß beschränkt; insuffiziente Umsetzung des Grundsatzes der Datenminimierung. • Verarbeitung von personenbezogenen Daten zu inkompatiblen Zwecken (zB Marketing via Metadaten)

	• Geringeres rechtliches Schutzniveau im Sitzstaat von Google (USA). Nach FISA 702 können US-amerikanische „Anbieter elektronischer Kommunikationsdienste“ (wie in 50 U.S.C. §1881(4) definiert), dazu gezwungen werden, den US-Sicherheitsbehörden Zugang zu den personenbezogenen Daten von "Nicht-US-Personen" zu gewähren.
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: gesellschaftliche und soziale Nachteile (durch weitere Monopolisierung privater IT-Konzerne), strukturelle Schädigung der Privatsphäre (Tracking über Webseiten, Applikationen und Endgeräte hinweg); Chilling Effects, wenn Menschen davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit zu entfalten

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Maximal (4) Kommentar: Das Risiko ist bereits eingetreten.	- Wesentlich (3)	- Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Verwaltungsprozesse stehen den Betroffenen nach wie vor auch analog ohne Smartphone zu Verfügung. • Reduktion der Dienste der genannten Drittanbietern auf ein funktional notwendiges Ausmaß, Sicherstellung, dass Sub-Services (wie zB die Analysefunktionen bei Google Push Notifications) nicht zur Anwendung kommen

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Wesentlich (3)	- Normal (9)

5.2.20 Zweckwidrige Verarbeitung durch Firebase Cloud Messaging

1) Risikoidentifikation	**Risikobeschreibung**
	Jede Signatur bzw Anmeldung löst mittels Firebase Cloud Messaging eine Verarbeitung personenbezogener Daten bei Google Inc. aus. Diese Verarbeitung ist der Anwendung „Digitales Amt“ zuordenbar. Die Verarbeitung findet in einem Drittland statt, zugunsten dessen kein Angemessenheitsbeschluss nach Art 45 DSGVO in Kraft ist. Es besteht das Risiko, dass Google von im Drittland ansässigen Behörden zur Offenlegung von Daten verpflichtet wird. Daneben besteht das Risiko, dass Google empfangene Daten selbst verarbeitet. Anmerkung: Soweit Betroffene iOS verwenden, ist dieses spezifische Risiko nicht einschlägig. Das Apple Notification Service erhält von Firebase Cloud Messaging (FCM) Anfragen zum Versand von Push Benachrichtigungen an iOS Benutzer*innen. Die an Apple weitergeleitete Push Benachrichtigung enthält keine empfänger*innenspezifischen und damit personenbezogenen Daten. Für die Zustellung (Network Layer) wird auf der Basis des Betriebssystems die IP-Adresse des Geräts verarbeitet. Das Risiko erschöpft sich daher im allgemeinen Systemrisiko von Apple Inc.
	Risikoquelle
	Externe menschliche Quellen: • Google (*Auftragsverarbeiter*) • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung)
	Risikoursache
	Google verarbeitet Firebase-Dienstdaten auch zu eigenen Zwecken[453] Geringeres rechtliches Schutzniveau im Sitzstaat von Google (USA). Nach FISA 702 können US-amerikanische „Anbieter elektronischer Kommunikationsdienste“ (wie in 50 U.S.C. § 1881(4) definiert) gezwungen werden, den US-Sicherheitsbehörden Zugang zu den personenbezogenen Daten von „Nicht-US-Personen“ zu gewähren.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Diskriminierung (zB bei Vertragsabschlüssen) **Immaterielle Schäden:** • Rufschädigung • Wirtschaftliche oder gesellschaftliche Nachteile • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

[453] Vgl https://firebase.google.com/support/privacy (abgerufen am 22. 04. 2022).

	• Körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten • Verletzung des Rechts auf informationelle Selbstbestimmung

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Wesentlich (3)	- Wesentlich (3)	- Normal (9)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Deaktivierung standardmäßiger Zusatzdienste (Analytics, Advertisement ID, Root-Detection) • Kein Einsatz externer Frameworks • Versendung über Google/Apple interne Services • Verwendung von Firebase ausschließlich für die Versendung von Push Notifcations • Der Einsatz von Firebase Cloud Messaging wird in der Datenschutzerklärung dargestellt; dem müssen Benutzer*innen zustimmen. Zudem wird auf Betriebssystemebene gefragt, ob Push Nachrichten gesendet werden sollen, was in den Systemeinstellungen jederzeit deaktiviert werden kann.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	- Eingeschränkt (2)	- Wesentlich (3)	- Normal (6)

5.3 Diskussion der verbleibenden Risiken und Folgenabschätzung

Die vorliegende Analyse zeigt, dass – nach Ermittlung und Zuordnung der bestehenden technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen – in der Umsetzung des ID Austria Systems nach derzeitigem Stand keine als hoch zu bewertenden Risiken bestehen.

Aufgrund des Tempos der technologischen Veränderung und der damit einhergehenden Möglichkeit der funktionalen Weiterentwicklung des E-ID Systems sind jedenfalls regelmäßig Überprüfungen durchzuführen, um zu bewerten, ob bzw inwiefern sich die mit der Datenverarbeitung verbundenen Risiken geändert haben und eine Anpassung der technischen und organisatorischen Maßnahmen erforderlich ist;[454] exemplarisch kann hier auf die geplante Implementierung des FIDO-Authentifizierungsverfahrens oder von Signaturkarten als Alternative zur Smartphone-Biometrie verwiesen werden. Die Umsetzung dieser Maßnahme ist bereits in Gang und erfolgt zeitnahe mit einem Update zur ID Austria. Der methodische Prozess der Risikoanalyse, -beurteilung und -behandlung wird auf derartige Entwicklungen auszudehnen und fortzusetzen sein, um damit das Vertrauen der Menschen zu rechtfertigen.

Sollte aus dieser Beurteilung künftig hervorgehen, dass Verarbeitungsvorgänge im Rahmen des E-ID Systems ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, ist gem Art 36 DSGVO die Aufsichtsbehörde zu konsultieren.[455]

Der Verantwortliche will ein solches Konsultationsverfahren, welches vor allem auch mit einem hohen Aufwand für die Datenschutzbehörde verbunden ist, auch künftig durch risikoangemessene, nachvollziehbare Anstrengungen in der Fortentwicklung vermeiden. Unabhängig davon soll die Datenschutzbehörde durch proaktive Vorlage dieses initialen DSFA-Berichts sowie künftig auch im Falle von Aktualisierungen stets fachlich qualifiziert auf dem Laufenden gehalten werden. Dabei gilt es – neben den hier geprüften und analysierten Risiken – gesamtgesellschaftliche Entwicklungen ebenfalls zu berücksichtigen.

So sind allfällige Tendenzen eines potenziellen gesellschaftlichen Ausschlusses oder einer möglichen Ungleichbehandlung als Folge des Technologieeinsatzes kritisch zu beobachten und durch entsprechende Maßnahmen zu adressieren. Dabei geht es insb um Konsequenzen für jene Personen bzw Bevölkerungsgruppen, welche die E-ID aus verschiedenen Gründen nicht verwenden möchten oder können.

Im Kern handelt es sich beim E-ID um einen staatlich generierten und zentral verwalteten Identitätsnachweis auf Basis und in Verbindung mit einer Reihe an behördlichen Registern und Sicherheitsdaten, der künftig grundsätzlich einer Vielzahl an Anwendungsmöglichkeiten offensteht. Neben den zahlreichen behördlichen Anwendungen steht hier vor allem die weitere Einbindung der E-ID in verschiedene Anwendungen privatwirtschaftliche Provider zur Diskussion. Derartige Entwicklungen sind jedenfalls weiterhin zu beobachten und sorgfältig auf ihre Zulässigkeit und Verhältnismäßigkeit zu prüfen. Hierbei ist auch darauf zu achten, dass die künftigen *Verantwortlichen*

[454] Siehe Art 5 Abs 2 sowie Art 35 Abs 11 DSGVO.
[455] Siehe ErwGr 84 DSGVO; vgl *Martin* et al, Datenschutz-Folgenabschätzung (2020) 49.

solcher privaten Angebote ihren datenschutzrechtlichen Pflichten nachkommen und bei Vorliegen hoher Risiken ebenfalls eine eigenständige Datenschutz-Folgenabschätzung zur jeweiligen Anwendung durchführen.

6 Fazit und getroffene Entscheidungen

Im Ergebnis zeigt die vorliegende DSFA, dass die identifizierten bzw verbleibenden Risiken aufgrund der gesetzten Maßnahmen des *Verantwortlichen* für die Betroffenen im Produkt ihrer Eintrittswahrscheinlichkeit und Schwere nicht als hoch einzustufen sind. Aus derzeitiger Sicht besteht somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Artikel 36 DSGVO. Die Notwendigkeit und Verhältnismäßigkeit der untersuchten Datenverarbeitungsprozesse werden auf Basis der entsprechenden systematischen Analyse in Verbindung mit den Rechtsgrundlagen und unter Berücksichtigung aller technischen und organisatorischen Maßnahmen als gegeben erachtet.

Zusammenfassend kann somit festgehalten werden, dass

- bereits die Architektur des ID Austria Systems dem „Privacy by Design“ Prinzip des Datenschutzrechts und damit auch dem Grundsatz der Datenminimierung folgt;
- die Protokollierung hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt ist;
- personenbezogene Daten stringenten Pseudonymisierungs- und Löschfristen unterliegen;
- personenbezogene Daten nur von berechtigten Stellen verarbeitet bzw übermittelt werden, soweit diese hierfür notwendig sind
- gespeicherte personenbezogene Daten strengen Zugriffsrechten unterliegen;
- nur die für die Zweckerfüllung erforderlichen Daten erhoben werden bzw sind im Registrierungs- und Anmeldeprozess nur Felder und Funktionen vorgesehen, die erforderlich sind.

Der DSFA-Bericht gelangt somit zu dem Ergebnis, dass es im ID Austria System eine Vielzahl an Garantien und Verfahren gibt, welche die Risiken der geplanten Verarbeitungsprozesse eindämmen sowie den Schutz personenbezogener Daten sicherstellen. Die Einhaltung aller datenschutzrechtlichen An-forderungen und Bestimmungen ist gewährleistet und wird durch diesen Bericht dokumentiert.

6.1 Ausblick

Die Europäische Kommission hat im Jahr 2021 nach einer Evaluierung der eIDAS-VO einen Entwurf für die Anpassung der Verordnung vorgelegt.[456] Dieser soll Änderungen und Erweiterungen in einigen Bereichen erwirken, um bestehende Schwächen des eIDAS-Regimes auszugleichen.[457] Demnach ist nicht auszuschließen, dass nach Inkrafttreten dieses Vorschlags aufgrund der unionsrechtlichen Vorgaben auch eine Anpassung des vorliegenden ID Austria Systems notwendig ist. Der Vorschlag zur Änderung der eIDAS-VO hat jedenfalls das Potential, die Nutzung elektronischer Identitäten im europäischen Binnenmarkt weiter zu fördern und voranzutreiben.[458]

[456] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats zur Änderung der Verordnung (EU) Nr. 910/2012 im Hinblick auf die Schaffung eines Rahmens für die europäische digitale Identität, COM (2021) 281 final 2021/0136 (COD), zur angesprochenen Evaluierung siehe insb Seite 1 f.

[457] Vgl Vorschlag für eine Verordnung, COM (2021) 281 final 2021/0136 (COD); vgl auch *OV (Europäische Kommission)*, Building a Trusted and Secure European Digital Identity, https://digital-strategy.ec.europa.eu/en/library/building-trusted-and-secure-european-digital-identity-brochure (abgerufen am 22. 04. 2022).

[458] *Ortalda/Tsakalakis/Jasmontaite*, The European Commission Proposal Amending the eIDAS Regulation (EU) No 910/2014: A Personal Data Protection Perspective, Brussels Privacy Hub (2021).

Darüber hinaus stehen in technischer Hinsicht internationale Diskussionen und Arbeiten wie etwa künftige Entwicklungen rund um das Konzept der „Self-Sovereign Identity“ (SSI) im Raum. Kerngedanke dieses Konzepts der selbstbestimmten digitalen Identität ist es, dass die E-ID ohne eine zentrale vermittelnde Instanz erzeugt und genutzt werden kann; damit wird die Autonomie der Nutzer*innen gefördert und die Kontrolle über die eigenen Identitätsdaten ermöglicht. Aus Sicht des *Verantwortlichen* ist die technische ebenso wie die rechtliche Architektur dieses Konzepts derzeit jedoch noch nicht genügend ausgereift. Es gibt sowohl wissenschaftliche als auch zivilgesellschaftliche Kritik,[459] auf die bislang keine hinreichenden Antworten gefunden wurden. Entsprechende Entwicklungen und Möglichkeiten werden durch den *Verantwortlichen* weiterverfolgt.[460]

6.2 Pflicht zur künftigen Überprüfung

Das ID Austria System unterliegt somit in rechtlicher wie auch technischer Hinsicht einer permanenten und mitunter volatilen Weiterentwicklung. Aufgrund dieses Umstands hat der *Verantwortliche* einen laufenden Abgleich des Soll-Zustands mit dem Ist-Zustand vorzunehmen und zu überprüfen, ob bzw inwiefern hinsichtlich der mit den Verarbeitungsvorgängen des ID Austria Systems verbundenen Risiken beachtliche Änderungen eingetreten sind. Die Pflicht einer derartigen Überprüfung ist nicht zuletzt auch in Art 35 Abs 11 DSGVO normiert. Lässt sich eine Änderung der Risikolage identifizieren, sind entsprechende Anpassungen der technischen und organisatorischen Maßnahmen für eine datenschutzkonforme Verarbeitung der personenbezogenen Daten vorzunehmen.

[459] *Pöhn/Grabatin/Hommel*, eID and Self-Sovereign Identity Usage: An Overview, electronics (2021) 10, 2811; vgl auch https://damienbod.com/2021/10/11/challenges-to-self-sovereign-identity/ (abgerufen am 22. 04. 2022).
[460] Siehe hierzu bspw die Diskussion in Deutschland unter https://www.bundesregierung.de/breg-de/suche/e-id-1962112 (abgerufen am 22. 04. 2022); siehe auch ENISA, Digital Identity – Leveraging the Self-Sovereignty Identity (SSI) Concept to Build Trust (2022).

Glossar und Abkürzungsverzeichnis

ABl:	Amtsblatt der Europäischen Union; („L" steht in diesem Zusammenhang für Rechtsakte, „C" für Mitteilungen und Bekanntmachungen und „S" für Ausschreibungen)[461]
Abs:	Absatz
AES 256-Bit-Verschlüsselung:	Advanced Encryption Standard (Chiffre)
Anm:	Anmerkung
API:	Programmierschnittstelle
APNs:	Apple Push Notification Service; Lösung für das Versenden von Push Notifcations auf Apple-Geräten[462]
Art:	Artikel
A-SIT:	Zentrum für sichere Informationstechnologie - Austria
Auftragsverarbeiter:	Legaldefinition gem Art 4 Z 8 DSGVO
bcBind:	Zertifikatsbindung, die für eine spätere vereinfachte Weiterverwendung der ID Austria verwendet werden kann
BerAbgrVo:	Bereichsabgrenzungsverordnung; E-Gov-BerAbgrVo: Verordnung des Bundeskanzlers, mit der staatliche Tätigkeitsbereiche für Zwecke der Identifikation in E-Government-Kommunikationen abgegrenzt werden, BGBl II 2004/289
BGBl:	Österreichisches Bundesgesetzblatt; „I" steht in diesem Zusammenhang für den ersten Teil, in dem Gesetze kundgemacht werden, in Teil „II" wiederum Verordnungen und in Teil „III" Staatsverträge
Bitkom:	Deutscher Bundesverband der Informationswirtschaft und Telekommunikationsbranche
bPK:	bereichsspezifisches Personenkennzeichen; dieses dient grundsätzlich der eindeutigen Identifikation von natürlichen Personen in einem konkreten Verwaltungsverfahren[463] und wird prinzipiell durch eine Ableitung aus der Stammzahl der betroffenen natürlichen Person gebildet, wobei die Identifizierungsfunktion auf jenen staatlichen Bereich begrenzt ist, dem die Datenverarbeitung zuzurechnen ist, in der das bPK verarbeitet werden soll (§ 9 Abs 1 E-GovG); dadurch soll sichergestellt werden, dass die Daten eines Verwaltungsbereichs über eine Person nicht mit einem anderen verknüpft werden können; die mathematischen Verfahren, die dabei eingesetzt werden (Hash-Verfahren über die Stammzahl und die Bereichskennung), werden von der Stammzahlenregisterbehörde festgelegt und im Internet veröffentlicht (§ 9 Abs 3 E-GovG); im privaten Bereich können uU ebenso bPKs gebildet werden,

[461] Siehe *Dax/Hopf*, Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europäische Rechtsquellen[8] (2019) 43.
[462] Vgl https://developer.apple.com/go/?id=push-notifications (abgerufen am 28.11.2021).
[463] Vgl *Feik/Randl* in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[3] (2012) 399.

	indem anstelle der Bereichskennung die Stammzahl oder das bPK des *Verantwortlichen* des privaten Bereichs verwendet wird (§ 14 Abs 1 E-GovG).
BlgNR:	Beilagen zu den stenographischen Protokollen des Nationalrates[464]
BMI:	Bundesminister für Inneres
BMDW:	Bundesminister für Digitalisierung und Wirtschaftsstandort
bPK-VDA:	Bereichsspezifisches Personenkennzeichen „Vertrauensdiensteanbieter“
bPK-ZP:	Bereichsspezifisches Personenkennzeichen „Zur Person“
BRZ:	Bundesrechenzentrum GmbH
BSI:	Bundesamt für Sicherheit in der Informationstechnik; deutsche Bundesbehörde
bsph:	beispielhaft
bspw:	beispielsweise
BStatG:	Bundesstatistikgesetz 2000; Bundesgesetz über die Bundesstatistik, BGBl I 1999/163
bzgl:	bezüglich
bzw:	beziehungsweise
Client-Komponente:	Entweder „Digitales Amt-App“, Third-Party-App oder Mobiler Web-Browser, die/der Signaturerstellungs-Requests erstellt, übermittelt und empfängt
CNIL:	französische Datenschutzbehörde
Dritter:	Legaldefinition gem § 18 Abs 1 Z 3 E-GovG sowie gem Art 4 Z 10 DSGVO
DSFA:	Datenschutz-Folgenabschätzung gem Art 35 DSGVO
DSFA-AV:	Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung, BGBl II 2018/108
DSFA-V:	Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, BGBl II 2018/278
DSG:	Datenschutzgesetz; Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, BGBl I 1999/165
DSGVO:	Datenschutz-Grundverordnung; VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, 1

[464] *Dax/Hopf*, AZR[8], 43.

EGIZ:	E-Government Innovationszentrum
EG-DSRL:	RL (EG) 95/46 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31
E-GovG:	E-Government-Gesetz; Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, BGBl I 2004/10
E-ID:	elektronischer Identitätsnachweis (siehe insb § 2 Z 10 E-GovG)
eIDAS-VO:	VO (EU) 910/2014 des Europäischen Parlaments und des Rats über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl L 2014/257, 73
E-ID-Werber:	Benutzer*in im Stadium des laufenden Registrierungsprozesses
E-ID-Inhaber:	Legaldefinition gem Art 4 Abs 2 E-GovG; Benutzer*in nach erfolgreichem Registrierungsprozess
Einschreiter:	Legaldefinition gem § 6 AVG
Empfänger:	Legaldefinition gem Art 4 Z 9 DSGVO
Erläut:	Erläuterungen
ErläutRV:	Erläuterungen zur Regierungsvorlage
ErläutIA:	Erläuterungen zum Initiativantrag
ERnP:	Ergänzungsregister natürlicher Personen
ERsB:	Ergänzungsregister für sonstige Betroffene
ErwGr:	Erwägungsgrund
EWR:	Europäischer Wirtschaftsraum
f/ff:	folgende(r/s)/fortfolgende
FCM:	Firebase Cloud Messaging; Lösung für das Versenden von Push Notifcations auf Android-Geräten[465]
ggf:	gegebenenfalls
GISA:	Gewerbeinformationssystem Austria
IA:	Initiativantrag
idF:	in der Fassung
IdP:	Identity Provider

[465] Vgl https://firebase.google.com/docs/cloud-messaging (abgerufen am 28.11.2021).

idR:	in der Regel
IDR:	Identitätsdokumentenregister
inkl:	inklusive
insb:	insbesondere
iSd:	im Sinne der/des
iSe:	im Sinne einer/eines
ISMS:	Information Security Management System
iSv:	im Sinne von
iZm:	im Zusammenhang mit
krit:	kritisch
lit:	litera/literae
LoA:	Level of Assurance
MDS:	Minimal Dataset (bestehend aus Vor- und Nachnamen sowie Geburtsdatum)
Nr:	Nummer
OIDC:	Open ID Connect
ÖNACE:	Österreichische Klassifikation der wirtschaftlichen Tätigkeiten („Nomenclature générale des activités économiques dans les communautés européennes“)
Personenbindung:	Dadurch wird dem *ID-Inhaber* von der SZRB elektronisch signiert oder besiegelt bestätigt, dass ihm ein oder mehrere bereichsspezifische Personenkennzeichen zugeordnet sind. Die Personenbindung wird bei öffentlichen SP und bei eIDAS mit dem Minimal Dataset (bestehend aus dem Vor-, Nachname und Geburtsdatum) sowie dem bPK, im Fall privater SP nur mit dem bPK ohne MDS, verbunden, wodurch die SZRB auch die Richtigkeit der Zuordnung bestätigt.
Portalverbund:	Der Portalverbund ermöglicht den Zugriff auf behördenübergreifende Webanwendungen und die Verwaltung der zugehörigen Rechte.[466]
PVP:	Portalverbundprotokoll; wird ua dazu verwendet, um auf das SPRS zuzugreifen
Rz:	Randziffer
S:	Satz
SAD:	Statistik-Austria-Domain
SAML 2.0:	Security Assertion Markup Language 2.0

[466] Siehe https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund (abgerufen am 22.04.2022).

SCC:	Standard Contractual Clauses (Standarddatenschutzklauseln)
Secure Element:	Dedizierte, separate, manipulationssichere Hardware zum Speichern kryptografischer Daten am Endgerät
SO:	Service Owner; der Begriff bezeichnet die für den Service Provider verantwortliche Organisation. Das kann eine Organisation des öffentlichen Sektors (zB ein Ministerium) oder auch ein privatwirtschaftliches Unternehmen sein. Ein Service Owner kann für eine beliebige Anzahl an Service Providern verantwortlich sein.
SP:	Service Provider; dies bezeichnet die Anwendung, die ein Service Owner anbietet.
SPRS:	Service Provider-Register-Service; dient Service Ownern bzw Service Providern zur Verwaltung ihrer Applikationen
SSI:	Self Sovereign Identity
SSL:	Secure Sockets Layer
Stammzahl:	eine Zahl, die einer betroffenen Person zu deren eindeutiger Identifikation zugeordnet und auch für die Ableitung von bereichsspezifischen Personenkennzeichen bestimmt ist.[467]
StF:	Stammfassung
STMV:	Standard- und Muster-Verordnung 2004 BGBl II 2004/312
SVV	Signatur- und Vertrauensdiensteverordnung BGBl II 2016/208
SZR:	Stammzahlenregister
SZRB:	Stammzahlenregisterbehörde; nach § 7 Abs 1 E-GovG idF BGBl I 2020/169 ist dies der Bundesminister für Digitalisierung und Wirtschaftsstandort.
TAN:	transaction number
TOM(s):	(geeignete) technische und organisatorische Maßnahmen gem DSGVO[468]
ua:	unter anderem
uE:	unseres Erachtens
UGB:	Unternehmensgesetzbuch; Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen, dRGBl 1897/219
URL:	Uniform Ressource Locator; im allgemeinen Sprachgebrauch auch etwa eine Internetadresse
USP:	Unternehmensserviceportal

[467] Vgl § 2 Z 8 E-GOVG.
[468] Siehe etwa Art 24, 32 DSGVO.

uU:	unter Umständen
VDA:	Vertrauensdiensteanbieter; Legaldefinition gem Art 3 Z 19 eiDAS-VO und § 3 (1) Z 2 Signatur- und Vertrauensdienstegesetz; ein Dienst, der elektronische Signaturen, Siegel oder Zertifikate erstellt, überprüft und validiert sowie aufbewahrt[469]
Verantwortlicher:	Legaldefinition gem Art 4 Z 7 DSGVO
vgl:	vergleiche
VO:	Verordnung
VStG:	Verwaltungsstrafgesetz 1991 BGBl 1991/52 (WV) idF BGBl I 1999/194
vSZ:	verschlüsselte Stammzahl; siehe zu dieser bereits oben
Z:	Ziffer
zB:	zum Beispiel
ZMR:	Zentrales Melderegister
ZMR-Zahl:	Melderegisterzahl; ein Meldedatum bzw Identitätsdatum gem § 1 Abs 5 bzw 5a Meldegesetz 1991, BGBl I 1992/9
Zsh:	Zusammenhang

[469] Siehe hierzu auch die Liste an Vertrauensdiensteanbietern unter https://www.rtr.at (abgerufen am 22. 04.2022).