

Digitaler Nachweis des Alters

Datenschutz-Folgenabschätzung

Research Institute – Digital Human Rights Center

DSFA-Bericht Digitaler Altersnachweis | 2023

<https://researchinstitute.at>

Digitaler Nachweis des Alters

Datenschutz-Folgenabschätzung

Bericht zur Datenschutz-Folgenabschätzung des digitalen Nachweises des Alters im Auftrag des Bundesministeriums für Finanzen (BMF)

Wien, September 2023

Autoren:

Christof Tschohl

Jan Hospes

Moritz W. Rothmund-Burgwall

Philipp Poindl

Walter Hötendorfer

Projektleitung:

Jan Hospes

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](https://twitter.com/researchinst)

© 2023 RI – Alle Rechte vorbehalten

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	12.07.2023	V 0.1	Erstellung der internen Berichtsstruktur	Jan Hospes	Berichtsstruktur
2	08.08.2023	V 0.3	Erste Version des Sachverhalts, der Rechtsgrundlagen und der Rollen festgehalten	Jan Hospes	in Arbeit
3	12.08.2023	V 0.4	Ausführungen zu Betroffenenrechten und Verarbeitungsgrundsätzen	Jan Hospes	in Arbeit
4	11.08.2023	V 0.5	Feedback und Ergänzungen seitens BMF und BRZ	Patrick Silli	Feedback
5	18.08.2023	V 0.6	Einbau letzter Erkenntnisse hinsichtlich Sachverhalt, Entwurf Risikobeurteilung	Jan Hospes	in Arbeit
6	22.08.2023	V 0.7	Einarbeitung Risikobeurteilung, Betroffenenrechte	Jan Hospes	in Arbeit
7	22.08.2023	V 0.7a	Ergänzungen und Bereinigungen seitens BMF nach Review	Patrick Silli	Feedback
8	22.08.2023	V 0.7b	Ergänzungen insb im Sachverhalt und betreffend Maßnahmen zur Einhaltung der DSGVO	Jan Hospes	in Arbeit
9	24.08.2023	V 0.8	Einarbeitung diverser Ergänzungen und Anmerkungen	Walter Hötzendorfer	Review
10	25.08.2023	V 1.0	Einarbeitung Review	Jan Hospes	Final

Disclaimer

Sofern im Folgenden nicht anders angegeben, wurden alle Internetlinks zuletzt am 23.08.2023 abgerufen.

Im Sinne eines diskriminierungsfreien Sprachgebrauchs ist der vorliegende Bericht mit * gegendert. Da einschlägige Gesetztexte 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.

Inhalt

1	Management Summary	8
2	Einleitung	10
2.1	Erforderlichkeit einer Datenschutz-Folgenabschätzung (Schwellwertanalyse)	11
3	Darstellung des Sachverhalts und Spezifizierung des Prüfgegenstands	12
3.1	Systemarchitektur.....	13
3.2	Prüfgegenstand.....	15
3.3	Die einzelnen Datenverarbeitungstätigkeiten	15
3.3.1	Altersnachweis laden und anzeigen	15
3.3.2	Alter nachweisen	17
3.3.3	Altersnachweis aktualisieren.....	20
4	Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge	21
4.1	Personenbezug.....	22
4.1.1	Was sind personenbezogene Daten?	22
4.1.2	Personenbezogene Daten im System	24
4.2	Rechtsgrundlagen	25
4.2.1	Regelungssystematik der DSGVO	25
4.2.2	Altersnachweis laden und anzeigen	26
4.2.3	Alter nachweisen	27
4.2.4	Altersnachweis aktualisieren.....	27
4.3	Rollenverteilung nach Maßgabe der DSGVO	27
4.3.1	Allgemeine Systematik der Rollenverteilung.....	27
4.3.2	Abgrenzungskriterien für die Ermittlung der (gemeinsam) Verantwortlichen	30
4.3.3	Altersnachweis laden und anzeigen	32
4.3.4	Alter nachweisen	34
4.3.5	Altersnachweis aktualisieren.....	34
4.4	Angaben über Maßnahmen zur Einhaltung der DSGVO	36
4.4.1	Grundsatz der Zweckbindung.....	36
4.4.2	Grundsatz der Datenminimierung.....	38
4.4.3	Grundsatz der Speicherbegrenzung	39
4.5	Angaben über die Berücksichtigung der Betroffenenrechte	39
4.5.1	Gewährleistung der Transparenz und Informationspflichten	39
4.5.2	Recht auf Auskunft und Datenübertragbarkeit.....	40
4.5.3	Recht auf Berichtigung und Löschung	40

4.5.4	Rechte auf Einschränkung und Widerspruch	41
4.5.5	Recht auf Beschwerde	41
4.6	Datenübermittlung in Drittländer (oder an internationale Organisationen)	42
4.7	Rat des Datenschutzbeauftragten und Standpunkt der Betroffenen.....	42
5	Datenschutzrechtliche Risikoabschätzung – Risk Assessment	44
5.1	Methodik.....	46
5.2	Risikobeurteilung	54
5.2.1	Unfreiwillige Nutzung des digitalen Altersnachweises.....	54
5.2.2	Diskriminierung aufgrund von Nicht-Nutzung des digitalen Altersnachweises	57
5.2.3	Unbefugter Zugriff auf IDR/ZMR/ERnP über das AWP-Backend	59
5.2.4	Protokollierung zu vieler personenbezogener Daten.....	61
5.2.5	Missbräuchliche Verwendung von Protokolldaten	62
5.2.6	Nichtverfügbarkeit des Systems	65
5.2.7	Vorweisen eines gefälschten digitalen Altersnachweises	68
5.2.8	Vorweisen einer faktisch unrichtigen Altersstufe	70
5.2.9	Vorweisen des Nachweises einer anderen Person.....	72
5.2.10	Rechtswidrige Verarbeitung durch Zugriffsbefugte	74
5.2.11	Auslesen des Nachweises ohne Rechtsgrundlage	76
5.2.12	Intransparenz der Datenverarbeitung.....	78
5.2.13	Nutzung der Ökosysteme von Google und Apple.....	80
5.3	Diskussion der verbleibenden Risiken und Folgenabschätzung	83
6	Fazit und getroffene Entscheidungen	84
6.1	Zusammenfassung der Ergebnisse.....	84
6.2	Pflicht zur künftigen Überprüfung	84
	Glossar und Abkürzungsverzeichnis	85

1 Management Summary

Der vorliegende Bericht dokumentiert die Ergebnisse der Datenschutz-Folgenabschätzung (DSFA) betreffend den digitalen Nachweis des Alters (folgend auch Altersnachweis). Der digitale Altersnachweis ist eine Funktion der Ausweisplattform, welche es Nutzer*innen ermöglicht, mittels der App eAusweise gegenüber anderen Nutzerinnen ihre Altersstufe nachzuweisen. Nutzer*innen haben somit künftig eine bedeutend datensparsamere Alternative dazu, etwa ihren Führerschein wie bisher in physischer Form oder nunmehr mittels eAusweise-App in digitaler Form vorweisen zu müssen, nur um das Alter nachzuweisen. Die Möglichkeit, physische Ausweise und Nachweise zu verwenden, bleibt wie bisher unverändert und uneingeschränkt bestehen.

Der digitale Altersnachweis baut auf der ID Austria und auf der Ausweisplattform auf. Zu beiden Systemen wurde gesondert eine DSFA durchgeführt und der DSFA-Bericht veröffentlicht.^{1 2}

Wenn der digitale Altersnachweis (so wie andere Ausweise/Nachweise auch) in der eAusweise-App geführt wird, erleichtert das den Nachweis ggü. Prüfern und Prüferinnen, sofern sie den digitalen Altersnachweis akzeptieren (Anm.: Ein Rechtsanspruch darauf besteht nicht). Nach dem Prinzip der Datenminimierung müssen Personen nur die wirklich relevanten Daten für den Altersnachweis offenlegen (also insb. nicht Namen und Geburtsdatum).

Der *Verantwortliche* hat entschieden, schon allein aufgrund der Bedeutung der vorliegenden Materie und der Bedeutung, die er dem Datenschutz beimisst, eine DSFA durchzuführen. Diese wurde durchgeführt und ist im vorliegenden Bericht dokumentiert.

Der Gegenstand der DSFA und somit auch der vorliegende Bericht gliedern sich in folgende Verarbeitungstätigkeiten:

- Altersnachweis laden und anzeigen;
- Alter nachweisen;
- Altersnachweis aktualisieren

Die Zulässigkeit und die Verhältnismäßigkeit dieser Verarbeitungstätigkeiten wurden beurteilt, wobei insbesondere auch auf die datenschutzrechtliche Rollenverteilung und Verantwortlichkeit eingegangen wurde.

Den Kern der DSFA bildet die datenschutzrechtliche Risikoanalyse, die eine Reihe von Risiken für die Rechte und Freiheiten der betroffenen Personen aufzeigt sowie diese Risiken und die diesbezüglich getroffenen Maßnahmen in methodisch systematischer Weise in ihrer Eintrittswahrscheinlichkeit und Schwere analysiert und bewertet. Dabei werden neben solchen Risiken, die mit nahezu jeder Verarbeitung personenbezogener Daten unweigerlich verbunden sind, insbesondere auch das Potenzial zur Überwachung und die dagegen getroffenen Maßnahmen behandelt sowie Fragen der Freiwilligkeit der Nutzung des Systems und das Thema einer möglichen Überforderung der betroffenen Personen, die Datenverarbeitung und ihre Konsequenzen zu verstehen.

¹ https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 24.08.2023).

² <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

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

Die vorliegende DSFA kommt zu dem Ergebnis, dass die identifizierten verbleibenden Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der gesetzten Maßnahmen des Verantwortlichen nicht als hoch einzustufen sind und somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Art 36 DSGVO besteht. 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

- personenbezogene Daten nur von berechtigten Stellen verarbeitet bzw übermittelt werden;
- nur die für die Zweckerfüllung erforderlichen Daten verarbeitet werden;
- personenbezogene Daten einem stringenten Löschkonzept unterliegen;
- gespeicherte personenbezogene Daten strengen Zugriffsbeschränkungen unterliegen;
- der Grundsatz der Datenminimierung und das Prinzip „Privacy by Design“ insbesondere durch die Implementierung des Vorweisens des digitalen Nachweises als Vorgang, der vollständig offline, ohne die Beteiligung eines Servers stattfindet, bereits in der grundlegenden Gestaltung des Systems berücksichtigt wurden;

Der DSFA-Bericht gelangt somit zu dem Ergebnis, dass eine Vielzahl von Garantien und Maßnahmen bestehen, welche die Risiken der geplanten Verarbeitungsprozesse eindämmen, den Schutz personenbezogener Daten sicherstellen sowie die Einhaltung aller datenschutzrechtlichen Anforderungen gewährleisten. Dies wird durch den vorliegenden Bericht dokumentiert.

Künftig gilt es die weitere technische, rechtliche und gesellschaftliche Entwicklung sorgfältig zu beobachten und die Auswirkung auf die Rechte und Freiheiten natürlicher Personen laufend zu prüfen. Dabei ist neben möglicher unbefugter Verarbeitung personenbezogener Daten insbesondere auf 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.

Den *Verantwortlichen* trifft 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.

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-Managementsystem 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.

2 Einleitung

Der vorliegende Bericht dokumentiert die Ergebnisse der durchgeführten Datenschutz-Folgenabschätzung (DSFA) zum digitalen Nachweis des Alters. Die DSFA dient insbesondere der Prüfung der damit verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung ihrer personenbezogenen Daten.

Zudem dient der vorliegende Bericht (neben der sonstigen Datenschutz-Dokumentation) als Nachweis der Einhaltung der Grundsätze des Datenschutzrechts (insb Rechenschaftspflicht gem Art 5 Abs 2 DSGVO im Rahmen der Verantwortung des für die Verarbeitung Verantwortlichen gem Art 24 Abs 1 DSGVO). Der Bericht dient auch ausdrücklich der Information der Öffentlichkeit; gegebenenfalls erfolgt eine Vorlage an den Datenschutzrat sowie an die österreichische Datenschutzbehörde.

Aus organisatorischer Sicht ist eingangs festzuhalten, dass die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) grundsätzlich der für die Datenverarbeitung verantwortlichen Stelle selbst obliegt. Als datenschutzrechtlich *Verantwortlicher* beauftragte das *Bundesministerium für Finanzen* (BMF) das *Research Institute – Digital Human Rights Center* (RI) im Juni 2023 mit der Unterstützung in der Ausarbeitung der vorliegenden Dokumentation zur Datenschutz-Folgenabschätzung (DSFA).

Die Beziehung des RI als externes Beratungsunternehmen stellt keine gänzliche Auslagerung, sondern vielmehr eine wesentliche fachliche Unterstützung dar, insbesondere bei der Dokumentation bereits während der Entwicklungsphase durchgeführter datenschutzrechtlicher Analysen und getroffener Maßnahmen. Ein wichtiges Ziel des Projekts war daher auch, eine systematische Konsolidierung der relevanten Dokumentation im Rahmen eines umfassenden DSFA-Berichts zu erreichen. In methodischer Hinsicht erfolgt die Ausarbeitung des DSFA-Berichts somit in enger Abstimmung mit dem *Verantwortlichen* und hat gewissermaßen 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.

Die Durchführung einer DSFA wird in methodischer Hinsicht als dynamischer Prozess verstanden. Aufgrund der ständigen Weiterentwicklung und Anpassung der in Rede stehenden IT-Systeme und Datenverarbeitungen ist somit auch künftig laufend zu prüfen, ob die bisherigen Ergebnisse noch gültig sind und der Risikobeurteilung standhalten. Dies sieht nicht zuletzt auch Art 35 Abs 11 DSGVO verpflichtend vor.

Kernbestandteil der hier dokumentierten DSFA ist die Risikobeurteilung. Für diese Schwerpunktsetzung spricht auch ErwGr 90 DSGVO, worin sinngemäß ausgeführt wird, dass sich eine Folgenabschätzung insbesondere mit den Maßnahmen, Garantien und Verfahren befassen sollte, durch die das Risiko der geplanten Verarbeitung eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden. Alle weiteren Ausführungen, insbesondere auch die sorgfältige Beschreibung der Verarbeitungsvorgänge sowie die Ebene der normativen Rechtfertigung, sind auch deswegen relevant, weil erst in diesem Kontext eine nachvollziehbare Risikobeurteilung durchgeführt werden kann.

2.1 Erforderlichkeit einer Datenschutz-Folgenabschätzung (Schwellwertanalyse)

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 insbesondere³ dann erforderlich, wenn eine

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet 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 Straftaten⁵ (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 zu veröffentlichen, für die eine DSFA verpflichtend durchzuführen ist („Blacklist“), und können zudem eine Liste mit Verarbeitungsvorgängen veröffentlichen, für die eine DSFA nicht verpflichtend ist („Whitelist“).⁶ Beides hat die österreichische Datenschutzbehörde getan.⁷

Nach der DSFA-AV („Whitelist“) sind Datenschutz-Folgenabschätzungen unter anderem dann nicht verpflichtend durchzuführen, wenn die Verarbeitung personenbezogener Daten⁸ im Rahmen von Registern, die durch Unions-, Bundes-, oder Landesrecht eingerichtet sind, erfolgt.⁹

Demgegenüber ist eine DSFA nach der sogenannten „Blacklist“ der DSB verpflichtend durchzuführen, wenn unter anderem¹⁰ 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.

Eine detaillierte Prüfung der Frage, ob im vorliegenden Fall eine DSFA verpflichtend durchzuführen ist, erübrigt sich, da der *Verantwortliche* entschieden hat, aufgrund der Bedeutung der Materie und der

³ Die Aufzählung dieser „Regelbeispiele“ ist also nicht abschließend: *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 36 (Stand 1. 9. 2019, rdb.at).

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 Berichtserstattung 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 Mit Ausnahme von Daten iSd Art 9 und 10 DSGVO.

⁹ DSFA-A06 Anlage 1 DSFA-AV.

¹⁰ Zusätzlich muss die Verarbeitung im Sinne der Art 6, 9 und 10 DSGVO rechtmäßig erfolgen und es darf andererseits kein Ausnahmetatbestand nach DSFA-AV vorliegen (§ 2 Abs 1 DSFA-V).

Bedeutung, die er dem Datenschutz beimisst, in jedem Fall eine DSFA durchzuführen. Diese wurde durchgeführt und ist im vorliegenden Bericht dokumentiert.

3 Darstellung des Sachverhalts und Spezifizierung des Prüfgegenstands

Der digitale Nachweis des Alters (folgend auch Altersnachweis) bietet Nutzer*innen die Möglichkeit, ihre Altersstufe(n) (z.B. älter als 18) einem Gegenüber nachzuweisen. Hierfür notwendige Daten werden in die eAusweise-App geladen und können vorgezeigt werden. Die prüfende Person nutzt ihrerseits die eAusweise-App oder die eAusweis-Check-App um die Daten zu verifizieren. Entsprechend baut der digitale Altersnachweis wesentlich auf der Architektur der Ausweisplattform des BMF auf und wird als spezifischer Verarbeitungszweck bzw. als eigenständige Funktion der Ausweisplattform beleuchtet.

Für das Laden und Speichern von Daten des digitalen Altersnachweises notwendige Daten werden über die ID Austria- geladen und als Attribute an die eAusweise-App übergeben. Die Daten dürfen dann offline gespeichert und verwendet werden wobei der Zeitpunkt der letzten Aktualisierung angezeigt wird.

3.1 Systemarchitektur

Die folgende Darstellung zeigt die Architektur des Systems und setzt die einzelnen Komponenten in Beziehung. Sie legt auch die Schnittstellen zu den Systemen ID Austria und Ausweisplattform offen, welche bereits in spezifischen Datenschutz-Folgenabschätzungen beleuchtet wurden.^{11 12}

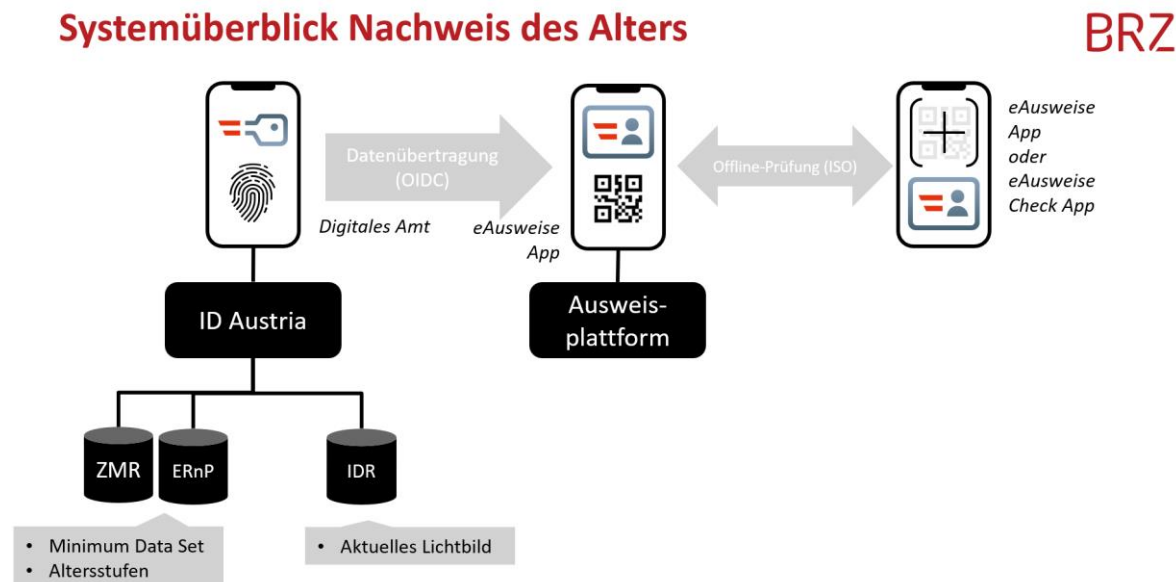


Abbildung 1: Überblick über die Funktionsweise der Funktion Altersnachweis basierend auf der eAusweise-App/Ausweisplattform und ID-Austria

Ausweisplattform (AWP)

Im Zuge der Realisierung der digitalen Ausweise wurde das System der Ausweisplattform entwickelt. Die Ausweisplattform stellt das serverseitige Herzstück des Systems dar, wie aus Abbildung 1 hervorgeht.

Digitaler Ausweis/ Nachweis

Ein digitaler Ausweis bzw digitaler Nachweis ist ein kryptographisch signiertes Set von Attributen einer Person. Diese Daten werden verschlüsselt in einer App auf einem Mobilgerät gespeichert (auch als "Wallet" bezeichnet). Dabei müssen digitale Aus- bzw Nachweise jedoch immer auch über einen elektronischen Prozess geprüft werden, eine reine Verwendung als Sichtausweis ist nicht möglich.

Digitales Amt App

Die App "Digitales Amt" fungiert aus Sicht der eAusweise-App als Frontend und User Interface der ID Austria. Für eine ID Austria-Anmeldung müssen sich Nutzer*innen in der App Digitales Amt biometrisch authentisieren und erforderlichenfalls in eine Datenübermittlung einwilligen.

eAusweise-App

¹¹ https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 24.08.2023).

¹² <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

Die eAusweise-App ermöglicht das Laden von Ausweisen auf ein mobiles Endgerät über die Ausweisplattform, das Vorweisen eines Ausweises/Nachweises mit der App und die Überprüfung eines Ausweises/Nachweises von einer anderen Person.

eAusweis Check-App

Um zum Überprüfen von Ausweisen nicht zwingend die (potentiell auch andere Funktionen enthaltende) eAusweise-App verwenden zu müssen, gibt es zusätzlich eine eigenständige Überprüfungs-App. Einziger Zweck dieser App ist die Überprüfung von Ausweisen, die eine andere Person mit ihrer eAusweise-App vorzeigt.

ID-Austria (IDA/IDP)

Das ID Austria-Backend führt alle notwendigen Operationen für eine ID Austria-Anmeldung durch und kommuniziert mit den jeweiligen Service Providern (hier die Ausweisplattform) über die Protokolle SAML 2.0 oder Open ID Connect.

IDR

Im Identitätsdokumentenregister (IDR) sind Daten gemäß § 22b Passgesetz 1992 gespeichert, insbesondere handelt es sich dabei um Reisepass- und Personalausweisdaten. Das aktuell im IDR jüngste Lichtbild wird für den digitalen Altersnachweis verwendet.

Minimum Data Set

Minimaler Datensatz der mit der ID Austria-Anmeldung übergeben wird (Vorname, Familienname, Geburtsdatum) sowie hier zusätzlich das bPK des staatlichen Tätigkeitsbereichs

Open ID Connect OIDC

Etablierter Standard zur Umsetzung von Identitätsmanagementsystemen und für die Interaktion zwischen Service Providern und Identity Providern

ISO

Die Übermittlung folgt dem internationalen Standard ISO/IEC 18013-5. Der Datenaustausch besteht hierbei aus drei Phasen: Initialisierung, Device Engagement und Data Retrieval

ZMR / ERnP

Das Zentrale Melderegister (ZMR) ist ein öffentliches Register, in dem alle in Österreich gemeldeten Personen mit ihrem Hauptwohnsitz und – sofern vorhanden – mit ihrem Nebenwohnsitz/ihren Nebenwohnsitzen erfasst sind. Im ZMR werden die Identitätsdaten (z.B. Name, Geschlecht, Geburtsdatum, ZMR-Zahl, Staatsangehörigkeit etc.) und die Wohnsitzdaten von Personen aufgenommen.¹³

Das Ergänzungsregister natürliche Personen (ERnP) ist ein Stammzahlenregister. Eine Stammzahl ermöglicht die eindeutige Identifikation einer digitalen Identität.¹⁴

¹³ <https://www.oesterreich.gv.at/lexicon/Z/Seite.991731.html> (abgerufen am 24.08.2023).

¹⁴ <https://www.oesterreich.gv.at/lexicon/E/Seite.991096.html> (abgerufen am 24.08.2023).

3.2 Prüfgegenstand

Gegenstand der vorliegenden DSFA sind daher die nachfolgend angeführten Verarbeitungstätigkeiten:

- **Altersnachweis laden und anzeigen;**¹⁵
- **Alter nachweisen;**¹⁶
- **Altersnachweis aktualisieren**¹⁷

Die angebenen Register (ZMR, ERnP, IDR) stellen keinen Gegenstand der vorliegenden DSFA dar, da diese unabhängig von Ausweisplattform und digitalem Altersnachweis der Verantwortlichkeit des jeweils zuständigen Bundesministeriums unterliegen. Zur Abgrenzung der verschiedenen datenschutzrechtlichen Verantwortlichkeiten im Detail siehe Abschnitt 4.3.

3.3 Die einzelnen Datenverarbeitungstätigkeiten

Im Folgenden wird eine funktionale Perspektive und vor allem die Perspektive der datenschutzrechtlich betroffenen Personen eingenommen, um den Gegenstand der vorliegenden DSFA und seine Komponenten, die oben bereits beschrieben wurden, in einzelne Verarbeitungstätigkeiten zu gliedern. Dies dient der Strukturierung des Untersuchungsgegenstandes aus datenschutzrechtlicher Sicht. Jedes der nachfolgenden Kapitel beschreibt eine Verarbeitungstätigkeit. Die darauffolgende datenschutzrechtliche Analyse folgt dieser Struktur.

3.3.1 Altersnachweis laden und anzeigen

Zweck dieser Verarbeitungstätigkeit ist es, für den Altersnachweis notwendige Daten auf das Endgerät der Nutzer*in zu laden. Das ist erforderlich, um den Altersnachweis vorzeigen zu können und somit eine Voraussetzung für die nachfolgend beschriebenen Verarbeitungstätigkeiten. Dazu wählt die Nutzer*in in der eAusweise-App nach biometrischer Authentifizierung die entsprechende Funktion zum Herunterladen des Altersnachweises auf das eigene Endgerät aus. Dazu springt die Benutzer*in in die „Digitales Amt App“, führt eine Anmeldung an der ID-Austria durch und bezieht ein Registrierungstoken (ID-Token) mittels dessen die Ausweisplattform Vorname, Familienname, Geburtsdatum, alle Altersklassen, Lichtbild, vbPK-VT, vbPK-ZP vom ID-Austria-System lädt. Die Ausweisplattform bereitet Altersklassen und Lichtbild als ISO-Struktur auf und übermittelt diese signiert an die eAusweise-App.¹⁸

Die wesentliche Information über erfolgte Verarbeitungsvorgänge, nämlich ob eine bestimmte betroffene Person ihren Altersnachweis auf ihr Endgerät geladen oder sich an der ID-Austria angemeldet hat, kann sich aus einem Protokolleintrag im jeweiligen System ergeben.¹⁹ Zu beachten ist zudem in diesem Zusammenhang, dass gemäß § 16a Abs 12 iVm § 14 Abs 5 MeldeG²⁰ aufseiten des zentralen Melderegisters bzw nach § 22b Abs 5 PassG²¹ für das Identitätsdokumentenregister – und somit außerhalb der Systemgrenzen der Ausweisplattform und der hierin darzustellenden Zuständigkeit des

¹⁵ Siehe dazu im Detail 3.3.1.

¹⁶ Siehe dazu im Detail 3.3.2.

¹⁷ Siehe dazu im Detail 3.3.3.

¹⁸ Die Signaturlaufzeit wird dabei an die Zertifikatslaufzeit der jeweiligen ID Austria angepasst.

¹⁹ Siehe zur Protokollierung der ID Austria 4.6 der DSFA zur ID-Austria sowie die DSFA zur Ausweisplattform <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

²⁰ Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 – MeldeG) BGBl I 1992/9 idF 2023/89.

²¹ Bundesgesetz betreffend das Passwesen für österreichische Staatsbürger (Passgesetz 1992) BGBl I 1992/839 idF 2021/123.

BMF – eine Protokollierung aller tatsächlich durchgeführten Verarbeitungsvorgänge und somit auch von Datenabfragen im Zuge des Ladens und von Aktualisierungen des Altersnachweises durchgeführt wird, aus der erkennbar ist, welcher Person welche Daten aus den soeben genannten Registern übermittelt wurden, wobei die Protokolldaten für drei Jahre aufzubewahren sind.

Geladene Daten werden ausschließlich im Filesystem der eAusweise-App am mobilen Endgerät verschlüsselt gespeichert, nicht jedoch serverseitig. Die Verschlüsselungsmethode wird durch das Endgerät der Nutzer*in vorgegeben. Die gängigen Betriebssysteme (Android/iOS) führen kein Cloud-Backup dieser Daten durch.

Lichtbild, geladene Altersstufen und Datum der letzten Aktualisierung können in der eAusweise-App gesichtet oder zur Prüfung vorgelegt werden.

Für das Laden des Altersnachweises ist die Installation der Digitales Amt App sowie eine aufrechte ID-Austria mit Vollfunktion oder eIDAS notwendig. Eine weitere Voraussetzung bildet das Vorliegen von Daten im Sinne von § 4 Z. 1 lit. a (die Information über das Erreichen einer bestimmten Altersgrenze) sowie § 4 Z. 2 lit. c (das aktuelle Lichtbild, ausgenommen das Lichtbild eines Reisepasses gemäß § 4a des Passgesetzes 1992) E-ID-Verordnung.

Die maximale Gültigkeit des Gerätezertifikats der eAusweise-App der Anwender*in beträgt 1 Jahr. Damit geht aus technischen Gründen eine identische Gültigkeitsdauer des digitalen Nachweises des Alters einher.

In der Folge werden in der eAusweise-App die Anwendungsfälle „Alter nachweisen“, „Details sehen“ und „Aktualisieren“ verfügbar.

Folgende Daten werden hierbei verarbeitet jedoch nicht am Endgerät gespeichert:

- Vorname urn:oid:2.5.4.42
- Familienname urn:oid:1.2.40.0.10.2.1.1.261.20
- Geburtsdatum urn:oid:1.2.40.0.10.2.1.1.55
- Ausstellerland
- bPK²²
- IP-Adresse des Mobilgeräts
- Status der ID Austria (Voll- oder Basisfunktion)
- Registrierungstoken (ID-Token)

Folgende Daten werden hierbei erhoben und am Endgerät gespeichert:

- Älter als 14 org.iso.18013.5.1:age_over_14
- Älter als 16 org.iso.18013.5.1:age_over_16
- Älter als 18 org.iso.18013.5.1:age_over_18
- Älter als 21 org.iso.18013.5.1:age_over_21

²² Die Ausweisplattform ist als öffentlicher Service Provider der ID-Austria iSv § 10 Abs 1 E-GovG berechtigt, sämtliche bPK abzufragen, die für die unterschiedlichen Aus- bzw Nachweise in der App notwendig sein könn(t)en. bPK, die nicht der Verantwortlichkeit des BMF unterliegen, werden dabei ausschließlich verschlüsselt (daher auch die Abkürzung vbPK) verarbeitet. Derzeit werden folgende bPK verarbeitet: vbPK VT (für Führerscheinregister); vbPK ZP (für Identitätsdokumentenregister), BPK ZP-MH (für AWP selbst).

- Aktuellstes Foto org.iso.18013.5.1:portrait
- Signaturzertifikat

3.3.2 Alter nachweisen

Zweck dieser Verarbeitungstätigkeit ist das Vorweisen und Überprüfen des Erreichens einer Altersstufe gegenüber einer prüfenden Nutzer*in der eAusweise-App²³ oder eAusweis-Check-App.

Die prüfende Person wählt in der eAusweise-App oder eAusweis-Check-App die Überprüfungsfunktion aus, und definiert welche Altersstufe überprüft werden soll. Hierbei kann zur Prüfung gestellt werden ob eine der definierten Altersstufen (14,16,18,21) schon erreicht oder gerade nicht erreicht wurde.

Welche Berechtigung möchten Sie prüfen?

Wählen Sie die Altersberechtigung, die Sie überprüfen möchten.

The screenshot displays three light blue rounded rectangular buttons stacked vertically. Each button contains the following text from top to bottom: a bolded age requirement, a descriptive subtitle, and a 'prüfen' button with a right-pointing arrow icon.

- ab 14**
Vollendetes 14. Lebensjahr
prüfen
- unter 16**
Vor dem 16. Geburtstag
prüfen
- ab 16**
Vollendetes 16. Lebensjahr
prüfen

Abbildung 2: Auswahl der zu prüfenden Altersstufe²⁴

Parallel öffnet die nachweisende Nutzer*in die eAusweise-App und wählt dort den Anwendungsfall "Alter nachweisen" aus. Daraufhin wird das letzte Aktualisierungsdatum und die Information, dass ein QR Code generiert wird, um eine Datenverbindung mit einem prüfenden Gerät aufzubauen, angezeigt. Die Nutzer*in bestätigt mit „QR-Code erstellen“ woraufhin ein QR-Code mit einem Einmal-Token bzw

²³ Die eAusweise-App ist biometrisch abgesichert. <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

²⁴ Die Abbildung enthält nicht alle auswählbaren Altersstufen.

Device Engagement Code (DEC) angezeigt wird. Dieser kann daraufhin zur Überprüfung vorgezeigt werden.

Die Übermittlung und Überprüfung folgen dabei dem internationalen Standard ISO/IEC 18013-5. Der Datenaustausch besteht hierbei aus drei Phasen: Initialisierung, Device Engagement und Data Retrieval.²⁵

Das Device Engagement erfolgt im vorliegenden Fall über einen QR-Code, dh die Device-Engagement-Daten werden als QR-Code entsprechend dem Standard ISO/IEC 18004 übermittelt. Der QR-Code enthält die standardisierte Device-Engagement-Struktur. Darin sind Informationen darüber enthalten, welche Data-Retrieval-Methoden, dh Methoden zur Übermittlung der eigentlichen Daten, zur Verfügung stehen. Im System der eAusweise-App kommt dafür stets Bluetooth low energy (BLE) zum Einsatz. Die Übertragung mittels BLE bedarf der Erteilung der Berechtigung für die hierfür technologisch erforderlichen Funktionen am Endgerät, dh die Berechtigung für Bluetooth und in Android erfordert diese wiederum auch die Berechtigung für den Standort. Die App greift jedoch nicht auf den Standort zu, dh sie verarbeitet keinerlei Standortdaten.

Nachdem dieser QR-Code durch die Prüfer*in gescannt wurde, wird die ausgewählte Altersstufe der geprüften Nutzer*in angezeigt und sie wird aufgefordert, die Altersstufe freizugeben, die Anfrage abzulehnen oder bekanntzugeben, dass sie die angeforderte Altersstufe nicht erreicht bzw. schon überschritten hat. Bei Freigabe beginnt die Phase Data Retrieval. Dazu bauen die involvierten Mobilgeräte eine verschlüsselte Verbindung über Bluetooth low energy auf und es werden die Daten vom Endgerät der sich ausweisenden Person auf jenes der überprüfenden Person übertragen. Zur Verschlüsselung dieser Verbindung kommt der Standard AES-256-GCM zum Einsatz und das entsprechende Schlüssel-paar wird jeweils über HKDF gemäß RFC 5869 erzeugt.²⁶ Der Vorgang kann vor jedem Schritt abgebrochen werden.

Anschließend werden die Daten verifiziert (die Signatur mit dem entsprechenden App-Zertifikat überprüft). Der überprüfenden Person wird schließlich neben dem Lichtbild die Information angezeigt, ob die ausgewählte Altersstufe erreicht wurde oder nicht erreicht wurde. Der gesamte Überprüfungsvorgang erfolgt offline, die mobilen Geräte benötigen hierzu keine Internetverbindung und dieser Vorgang wird somit auch serverseitig nicht erfasst. Es werden keine personenbezogenen Daten der überprüfenden Person verarbeitet.²⁷

²⁵ Siehe INTERNATIONAL STANDARD ISO/IEC 18013-5 First edition 2021-09, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (6.3.2.1).

²⁶ Siehe zur Verschlüsselung insgesamt insb: INTERNATIONAL STANDARD ISO/IEC 18013-5 First edition 2021-09, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.

²⁷ <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

Altersnachweis Offline-ISO-Überprüfung (Bluetooth Low Energy)

BRZ

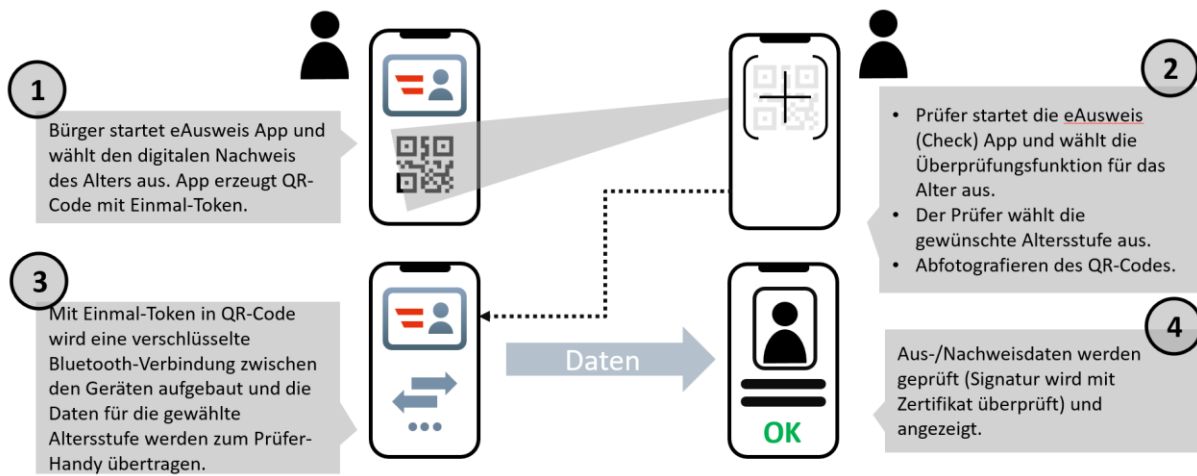


Abbildung 3: Ablauf des Nachweisvorgangs offline

Ist die Person über 16 ?

ALTERSBERECHTIGUNG PRÜFEN

JA

BERECHTIGUNG ERFÜLLT



07.07.2022 16:29

AKTUALISIERT AM

Ist die Person über 16 ?

ALTERSBERECHTIGUNG PRÜFEN

NEIN

BERECHTIGUNG: NICHT ERFÜLLT



07.07.2022 16:29

AKTUALISIERT AM

Berechtigung prüfen

Sie können die Prüfung der Altersberechtigung nun abschließen.

Prüfung abschließen

Berechtigung prüfen

Sie können die Prüfung der Altersberechtigung nun abschließen.

Prüfung abschließen

Abbildung 4: Prüfungsergebnis positiv (links) und negativ (rechts)

Folgende funktionspezifische Daten werden hierbei verarbeitet:

- Eine der folgenden Altersstufen:-
 - Älter als 14 org.iso.18013.5.1:age_over_14
 - Älter als 16 org.iso.18013.5.1:age_over_16
 - Älter als 18 org.iso.18013.5.1:age_over_18
 - Älter als 21 org.iso.18013.5.1:age_over_21
- Aktuellstes Foto org.iso.18013.5.1:portrait
- Signaturzertifikat

3.3.3 Altersnachweis aktualisieren

Zweck dieser Verarbeitungstätigkeit ist es, die Gültigkeit des (eigenen) digitalen Altersnachweises (mit allen Altersstufen) zu aktualisieren. Dies kann nach relevantem Geburtstag oder zur Verlängerung vor Ablauf der Gültigkeit relevant werden. Der Nutzer*in werden nach Auswahl der Funktion Informationen eingeblendet und wird in die App „Digitales Amt“ geleitet. Dort erfolgt eine Anmeldung an der ID-Austria und Daten werden entsprechend der Funktion „Altersnachweis laden und anzeigen“ (siehe 3.3.1) neu geladen.

Mein Altersnachweis

Digitaler Nachweis des Alters



21.06.2023, 13:23

AKTUALISIERT AM

Abbildung 5: Anzeige des Aktualisierungsdatums

Folgende Daten werden hierbei verarbeitet jedoch nicht am Endgerät gespeichert:

- Vorname urn:oid:2.5.4.42
- Familienname urn:oid:1.2.40.0.10.2.1.1.261.20
- Geburtsdatum urn:oid:1.2.40.0.10.2.1.1.55
- Ausstellerland

- bPK²⁸
- IP-Adresse des Mobilgeräts
- Status der ID Austria (Voll- oder Basisfunktion)

Folgende Daten werden hierbei erhoben und am Endgerät gespeichert:

- Älter als 14 org.iso.18013.5.1:age_over_14
- Älter als 16 org.iso.18013.5.1:age_over_16
- Älter als 18 org.iso.18013.5.1:age_over_18
- Älter als 21 org.iso.18013.5.1:age_over_21
- Aktuellstes Foto org.iso.18013.5.1:portrait

4 Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Im vorliegenden Kapitel wird dokumentiert, woraus sich die Zulässigkeit, Erforderlichkeit und Verhältnismäßigkeit der oben dokumentierten Verarbeitungsvorgänge im Sinne der einschlägigen Bestimmungen der DSGVO und des DSG ergibt.

Für die Verhältnismäßigkeits- und Erforderlichkeitsprüfung ist 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.²⁹

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 Abs 1 lit b);
- Rechtmäßigkeit der Verarbeitung (Art 6);
- Daten, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind (Art 5 Abs 1 lit c);
- begrenzte Speicherfrist (Art 5 Abs 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 (Art 18, 19 und 21);

²⁸ Die Ausweisplattform ist als öffentlicher Service Provider der ID-Austria iSv § 10 Abs 1 E-GovG berechtigt, sämtliche bPK abzufragen, die für die unterschiedlichen Aus- bzw Nachweise in der App notwendig sein könn(t)en. bPK, die nicht der Verantwortlichkeit des BMF unterliegen, werden dabei ausschließlich verschlüsselt (daher auch die Abkürzung vbPK) verarbeitet. Derzeit werden folgende bPK verarbeitet: vbPK VT (für Führerscheinregister); vbPK ZP (für Identitätsdokumentenregister), BPK ZP-MH (für AWP selbst).

²⁹ Vgl *Trieb* in *Knyrim*, *DatKomm* Art 35 Rz 112; siehe auch *Bock et al*, *Datenschutz-Folgenabschätzung für die Corona-App* (2020) 60 ff.

- Verhältnis zu Auftragsverarbeitern (Art 28);
- Garantien in Bezug auf die internationale Übermittlung von Daten.³⁰

4.1 Personenbezug

4.1.1 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 DSGVO fallen darunter auch pseudonymisierte Daten.

Die Definition des Begriffs „personenbezogene Daten“ ist somit sehr weit gefasst, denn es werden dem Wortlaut zufolge alle Informationen, die sich auf eine natürliche Person beziehen, davon umfasst.³¹ 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.³² 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.³³

Vor allem auch in Bezug auf Datenverarbeitungen durch Endgeräte wie Smartphones und Tablets, ist zu berücksichtigen, dass Standortinformationen, eindeutige Geräte- und Kundenkennungen (wie zB IMEI³⁴, IMSI³⁵, UDID³⁶, MSISDN³⁷), die Identität des Telefons³⁸, Kreditkarten- und Zahlungsdaten oder auch der Browserverlauf als personenbezogene Daten zu werten sind.³⁹ Weitere gängige Angaben mit identifizierendem Bezug zu einer natürlichen Person sind zB Handynummer⁴⁰, E-Mail-Adresse, Sozialversicherungsnummer⁴¹, KFZ-Kennzeichen⁴², IP-Adresse⁴³ und auch medizinische Diagnosen.⁴⁴

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.⁴⁵ Die Information kann sich zusammensetzen aus sachbezogenen Aussagen zu Verhältnissen oder

³⁰ 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.

³¹ Hödl in *Knyrim*, *DatKomm* Art 4 Rz 9 DSGVO (Stand 1. 12. 2018, rdb.at).

³² Klar/Kühling in *Kühling/Buchner*, *DS-GVO*² Art 4 Nr 1 Rz 8.

³³ Klar/Kühling in *Kühling/Buchner*, *DS-GVO*² Art 4 Nr 1 Rz 8.

³⁴ *International Mobile Equipment Identity* – eindeutige Nummer des Endgeräts.

³⁵ *International Mobile Subscriber Identity* – eindeutige Nummer des Netzteilnehmers.

³⁶ *Unique Device Identifier* – eindeutige Gerätenummer für Apple-Produkte.

³⁷ *Mobile Station Integrated Services Digital Network* – weltweit eindeutige Mobilfunk-Rufnummer.

³⁸ Nutzer*innen von Endgeräten können diese idR auch selbst benennen, wobei sie zumeist unter Verwendung ihres eigenen Namens benannt werden, wie zB „Maximilian Musterfrau iPhone“.

³⁹ *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, WP 202 (2013) 10 f.

⁴⁰ *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013, 10.

⁴¹ Vgl DSK 12. 11. 2004, K120.902/0017-DSK/2004; BVwG 11.06.2018, W211 2161456-1.

⁴² Vgl VfGH 15. 6. 2007, G 147/06; DSK 11.7.2008, K121.359/0016-DSK/2008.

⁴³ Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.

⁴⁴ Hödl in *Knyrim*, *DatKomm* Art 4 Rz 9 DSGVO.

⁴⁵ Vgl *Klabunde* in *Ehmann/Selmayr*, *DS-GVO*² Art 4 Rz 8.

überprüfbareren 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 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 als „*primäres Identifikationsmerkmal*“ bezeichnet.⁴⁶ 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.⁴⁷ 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 DSGVO 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.*“

⁴⁶ Vgl EuGH C-582/14, Breyer, ECLI:EU:C:2016:779.

⁴⁷ Klar/Kühling in Kühling/Buchner, DS-GVO/BDSG² Art 4 Nr 1 Rz 18; Eßer in Eßer/Kramer/v.Lewinski, DSGVO/BDSG⁷ Art 4 Rz 17.

Die Literatur⁴⁸ und unionsrechtliche Judikatur⁴⁹ setzen am sogenannten „*relativen Personenbezug*“ bzw der „*relativen Theorie*“⁵⁰ an, wonach für die Bestimmung der Identifizierbarkeit die Kenntnisse und Mittel der datenverarbeitenden Stelle und nicht irgendeines *Dritten* ausschlaggebend sind. Sofern der *Verantwortliche* Einzelangaben einer Person durch relevantes Zusatzwissen⁵¹ [ggf auch von ihm zurechenbaren (Sub-)Auftragsverarbeitern] direkt zuordnen kann, ist die Identifizierbarkeit zu bejahen, wodurch diese Einzelangaben für die datenverarbeitende Stelle als personenbezogene Daten gem Art 4 Z 1 DSGVO zu qualifizieren sind.⁵² Selbige Auffassung vertrat der EuGH in der Rechtssache C-582/14 zum Urteil *Breyer* gegen BRD, wonach dynamische IP-Adressen einer natürlichen Person für den Anbieter 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.*⁵³

4.1.2 Personenbezogene Daten im System

Nach dem Gesagten ist im gegenständlichen Fall daher grundsätzlich, insb sofern nichts Gegenteiliges beschrieben wurde, bei allen unter den Verarbeitungstätigkeiten (Kapitel 3.3) aufgelisteten Datenkategorien von personenbezogenen Daten auszugehen, zumal die datenverarbeitende Stelle in aller Regel einen Personenbezug im Sinne der Ausführungen dieses Kapitels herstellen können wird.

Anzumerken ist in diesem Zusammenhang außerdem, dass der Personenbezug von Daten auch durch ein Verschlüsselungsverfahren nicht geschmälert wird, weil die datenverarbeitende Stelle auch weiterhin den Personenbezug herstellen kann.⁵⁴ 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 wesentlich erschwert,⁵⁵ und daher zum Schutz personenbezogener Daten wesentlich beiträgt. Dementsprechend sind im gegebenen Fall jedenfalls auch verschlüsselte Daten, soweit solche unter 3.3 beschrieben wurden, als personenbezogene Daten anzusehen.

Darüber hinaus wäre es nicht sinnvoll, etwaige nicht personenbezogene Daten im Rahmen dieser DSFA anders zu behandeln als personenbezogene Daten, zumal eine Unterscheidung nur einen zusätzlichen Aufwand bedeuten würde und insb im Hinblick auf mögliche Maßnahmen zur Risikomitigierung auch nicht zweckmäßig erscheint.

⁴⁸ Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG⁷ Art 4 Rz 20; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 14; eher für die relative Theorie, allerdings teils differenzierte Ansicht *Ziebarth* in *Sydow*, Europäische Datenschutzgrundverordnung² Art 4 Rz 33 ff.

⁴⁹ Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.

⁵⁰ Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 14; *Klar/Kühling* in *Kühling/Buchner* DS-GVO/BDSG² Art 4 Nr 1 Rz 26 ff; *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG⁷ Art 4 Rz 20.

⁵¹ 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).

⁵² Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG⁷ Art 4 Rz 20.

⁵³ EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779, Rz 65.

⁵⁴ *Klabunde* in *Ehmann/Selmayr*, DS-GVO² Art 4 Rz 19.

⁵⁵ *Klabunde* in *Ehmann/Selmayr*, DS-GVO² Art 4 Rz 19.

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 rechtfertigt die betreffende Datenverarbeitung.⁵⁶ Für die vorliegende Verarbeitung von personenbezogenen Daten gem Art 4 Z 1 DSGVO enthält Art 6 Abs 1 DSGVO eine taxative Liste von sechs Erlaubnistatbeständen:

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

Art 9 Abs 2 DSGVO enthält die taxative Liste jener zehn Erlaubnistatbestände, auf welche die Verarbeitung besonderer Kategorien personenbezogener Daten⁵⁷ (kurz: sensibler Daten) gestützt werden kann.

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

⁵⁶ Vgl Feiler/Forgó, EU-DSGVO Art 6 Anm 1.

⁵⁷ Gem Art 9 Abs 1, Art 4 Z 13 - 15 DSGVO.

Im Folgenden ist dokumentiert, auf welche dieser Erlaubnistatbestände die Zulässigkeit der einzelnen oben angeführten Verarbeitungstätigkeiten gestützt wird.

4.2.2 Altersnachweis laden und anzeigen

Die Datenverarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationale Rechtsgrundlage für die Anmeldung an der ID-Austria bilden die §§ 4 iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG.⁵⁸

Die nationalen Rechtsgrundlagen für die Übermittlung von Altersstufen und Lichtbild bilden die §§ 4 Abs 6 E-GovG iVm § 4 E-ID-Verordnung. Vor der Übermittlung wird gemäß § 4 Abs 2 E-GovG die Einwilligung der betroffenen Person eingeholt. Grundlage für den Erlass der E-ID-Verordnung bilden die §§ 4a Abs. 6, § 18 Abs. 3 und 4 sowie § 25 Abs. 3 des E-Government-Gesetzes (E-GovG), wobei hinsichtlich des vorliegend einschlägigen § 4 E-ID-Verordnung § 18 Abs 4 E-GovG maßgeblich ist.

So kann nach § 4 Abs 1 lit a E-ID-Verordnung die Information über das Erreichen einer bestimmten Altersgrenze aus dem Zentralen Melderegister (ZMR) gemäß § 16a Abs. 4 des Meldegesetzes und gemäß § 4 Abs 2 lit c E-ID-Verordnung das aktuelle Lichtbild, ausgenommen das Lichtbild eines Reisepasses gemäß § 4a des Passgesetzes 1992, aus dem Identitätsdokumentenregister (IDR) an den E-ID-Inhaber übermittelt werden.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien⁵⁹ aus:

„In § 4 Abs. 6 wird klargestellt, dass der E-ID-Inhaber die Möglichkeit haben soll, Namen und Geburtsdatum in vereinfachter Form nachweisen zu können.“

Besonders zur Verordnungsermächtigung nach § 18 Abs 4 E-GovG:

„Aus Sicht des Bundesministeriums für Inneres ist es erforderlich, die Verordnungsermächtigung insoweit zu ergänzen, als insbesondere die für eine Registrierung gemäß Abs. 2 in Frage kommenden weiteren Dritten sowie die für die Nutzung zu verrechnenden Kostenersätze in der Verordnung näher zu bestimmen sind.

In Abs. 4 soll klargestellt werden, dass es für die Übermittlung der für die Nutzung des E-ID-Systems offenstehenden Datenarten zusätzlich zu Abs. 1 einer diesbezüglichen Rechtsgrundlage im jeweiligen Materiengesetz bedarf. Mit der vorgeschlagenen Verordnungsermächtigung soll ermöglicht werden, dass der für die jeweilige Datenverarbeitung zuständige Bundesminister die für eine Übermittlung gemäß Abs. 1 in Betracht kommenden Datenarten mit Verordnung konkretisieren kann, wobei sich jedoch die Rechtsgrundlage für die Datenübermittlung bereits aus einer gesetzlichen Regelung ergeben muss. Für eine Übermittlung gemäß Abs. 1 kommen lediglich Identitätsdaten (z. B. Vor- und Familiennamen sowie Geburtsdatum), Informationen zu Berechtigungen eines Betroffenen (z. B. Daten eines Reisedokumentes) oder Umstände, die der Betroffene nachweisen möchte (z. B. Hauptwohnsitz) in Betracht. Der Bundesminister für Inneres könnte beispielsweise die aus dem ZMR für die Verwendung der Funk-

⁵⁸ Siehe genauer Punkt 4.2.3 der DSFA betreffend ID-Austria unter: https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 24.08.2023).

⁵⁹ ErläutRV 469 BlgNR 27. GP 3, 8.

tion E-ID zur Verfügung stehenden Datenarten, die gemäß § 16a Abs. 4 MeldeG an die Stammzahlenregisterbehörde zur Erfüllung der gesetzlich übertragenen Aufgabe in Abs. 1 übermittelt werden, durch Verordnung präzisieren.“

4.2.3 Alter nachweisen

Die Datenverarbeitung stützt sich seitens des BMF zu Zwecken der Bereitstellung der Funktion auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationale Rechtsgrundlage bildet § 4 Abs 6 E-GovG.

Die überprüfende Person verarbeitet die personenbezogenen Daten der überprüften Person als eigenständige Verantwortliche. Sie hat ihre Rechtsgrundlage eigenverantwortlich im Einzelfall zu bestimmen. Ob diese Pflicht gegebenenfalls entfallen kann, weil die Überprüfung im Rahmen persönlicher oder familiärer Tätigkeiten iSd Art 2 Abs 2 lit c DSGVO erfolgt und die DSGVO daher nicht anwendbar ist, kann ebenfalls nur im Einzelfall geprüft werden.

4.2.4 Altersnachweis aktualisieren

Die Verarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO. Die Aktualisierung stützt sich als technisch gleichgelagerter Unterfall der Funktion „Altersnachweise laden und anzeigen“ auf §§ 4 Abs 6 E-GovG iVm § 4 E-ID-Verordnung. Die Anmeldung an der ID-Austria stützt sich auf die §§ 4 iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG. Genauere Angaben sind Punkt 4.2.1 zu entnehmen.

4.3 Rollenverteilung nach Maßgabe der DSGVO

4.3.1 Allgemeine Systematik der Rollenverteilung

Grundlegend festzuhalten ist, dass die Eruiierung der jeweiligen datenschutzrechtlichen Rolle eines datenverarbeitenden Akteurs 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;⁶⁰ dies trifft *vice versa* auch auf alle anderen Rollen zu.

Allgemein lässt sich die grundlegende Systematik der Rollenverteilung nach Maßgabe der DSGVO wie folgt überblicksartig zusammenfassen, wobei auf die Rolle des und der gemeinsam Verantwortlichen, Auftragsverarbeiter sowie der betroffenen Person teils näher eingegangen wird:

An oberster Stelle der Verantwortungskette bestimmt und wacht der Verantwortliche (oder die gemeinsam Verantwortlichen) als „Herr der Daten“⁶¹ über die Verarbeitung personenbezogener Daten natürlicher Personen, 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.⁶²

⁶⁰ Vgl Hödl in Knyrim, DatKomm Art 4 Rz 89.

⁶¹ Raschauer in Sydow, Europäische Datenschutzgrundverordnung² Art 4 Rz 123.

⁶² Vgl Hödl in Knyrim, DatKomm Art 4 Rz 83 f.

Sofern jedoch zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, führt dies zur sogenannten „*pluralistische[n] Kontrolle*“⁶³ über die jeweilige Datenverarbeitungstätigkeit, womit die gemeinsame Verantwortlichkeit nach Maßgabe von Art 26 DSGVO begründet ist.

Infolgedessen haben die gemeinsam Verantwortlichen eine Vereinbarung gem Art 26 Abs 1 und 2 DSGVO zu treffen, welche auch als „*Joint-Controller-Vereinbarung*“⁶⁴ 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 wer von den Verantwortlichen welche Verpflichtungen nach der DSGVO zu erfüllen hat,⁶⁵ wobei besonders wesentlich hierbei die Erfüllung der Informationspflichten gem Art 13 und 14 DSGVO ist.

Das Wesentliche dieser Vereinbarung muss den Betroffenen gem Art 26 Abs 2 Satz 2 DSGVO zur Verfügung gestellt werden, wobei dies am praktikabelsten gemeinsam mit den datenschutzrechtlichen Informationen gem Art 13 oder 14 DSGVO erfolgt.⁶⁶

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*⁶⁷
- *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,*⁶⁸
- *gegebenenfalls Benennung eines Verantwortlichen als zentrale Anlaufstelle nach Art 26 Abs 1 S 3.*⁶⁹

⁶³ *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 10, 22, 38f; *Hödl* in *Knyrim*, *DatKomm* Art 4 Rz 80.

⁶⁴ EuGH C-210/16 VbR 2018/109; *Gabauer/Knyrim*, Checkliste Prüfschema zur datenschutzrechtlichen Rollenverteilung, *Dako* 2019/8, 14 (15).

⁶⁵ *Veil* in *Gierschmann/Schlender/Stentzel/Veil*, *DS-GVO* Art 26 Rz 64.

⁶⁶ Vgl *Feiler/Forgó*, *EU-DSGVO* Art 26 Anm 3.

⁶⁷ *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.

⁶⁸ *Horn* in *Knyrim*, *DatKomm* Art 26 Rz 41 unter Verweis auf *Veil* in *Gierschmann/Schlender/Stentzel/Veil*, *DS-GVO* Art 26 Rz 64.

⁶⁹ *Horn* in *Knyrim*, *DatKomm* Art 26 Rz 41.

An der jeweiligen Verarbeitung kann auch ein **Auftragsverarbeiter** mitwirken, der dem *Verantwortlichen* stets als „*verlängerter Arm*“⁷⁰ dient. Dies, da der *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, als rechtlich eigenständige und externe Organisation,⁷¹ Datenverarbeitungstätigkeiten lediglich „im Auftrag“ des *Verantwortlichen* durchzuführen hat. Daher kommt dem *Auftragsverarbeiter* grds keine Entscheidungsbefugnis hinsichtlich der Verarbeitungszwecke und (wesentlichen) -mittel zu.⁷² Allerdings kann der *Verantwortliche* dem *Auftragsverarbeiter* bezüglich der Wahl von technisch 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.⁷³ Jedoch liegt die Entscheidungskompetenz über die „wesentlichen Mittel“ der Verarbeitung stets beim *Verantwortlichen*.⁷⁴

Die dem *Verantwortlichen* oder *Auftragsverarbeiter* unterstellten Personen gelten grds als ihnen „*zurechenbare Personen*“⁷⁵, da sie idR nur als „*Ausführungsorgan*“ für den *Verantwortlichen* oder *Auftragsverarbeiter* tätig sind.⁷⁶ Dies gilt jedoch nur solange sie sich an die Vorgaben bzw vorab festgelegten Zwecke und Mittel der Verarbeitung halten.

Zum **Empfänger** gem Art 4 Z 9 DSGVO zählt potenziell fast jeder datenverarbeitende Akteur,⁷⁷ der zumindest ein „gewisses Maß an Eigenständigkeit“⁷⁸ aufzuweisen hat und dem personenbezogene Daten innerhalb einer Verarbeitungstätigkeit lediglich offengelegt werden.

Ferner gibt es auch die Rolle des „außenstehenden“⁷⁹ **Dritten**, der bei Umgang mit personenbezogenen Daten selbst zu einem *Verantwortlichen* wird.

Die Rolle des „**Betroffenen**“ bzw 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.⁸⁰ Es kann daher jeder lebende⁸¹ Mensch die Rolle der betroffenen Person einnehmen, unabhängig von einer spezifischen Voraussetzung iS eines bestimmten Alters oder Geisteszustands.⁸²

⁷⁰ *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter – was ändert sich mit der DSGVO? ZTR 2017, 59 (59).

⁷¹ *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 30.

⁷² Vgl *Hödl* in *Knyrim*, *DatKomm* Art 4 Rz 94.

⁷³ *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.

⁷⁴ *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 17 f.

⁷⁵ 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.

⁷⁶ *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), *jusIT Spezial: DS-GVO* (2018), 31 (38).

⁷⁷ 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 bspw angeführt: „*Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, (...)*“

⁷⁸ 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.

⁷⁹ Vgl *Ernst* in *Paal/Pauly*, DS-GVO/BDSG² Art 4 Rz 59; *Buder* in *Jahnel* (Hrsg), *Datenschutzrecht*, 97 (136).

⁸⁰ *Hödl* in *Knyrim*, *DatKomm* Art 4 Rz 6; *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), *jusIT Spezial: DS-GVO* (2018), 31 (35).

⁸¹ Vgl ErwGr 27 und 158 Satz 1 DSGVO.

⁸² *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), *jusIT Spezial: DS-GVO* (2018), 31 (35).

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.⁸³ Darüber hinaus wurde in ErwGr 14 Satz 2 DSGVO weiters klargestellt, dass Daten, welche sich auf juristische Personen beziehen, grundsätzlich nicht vom Anwendungsbereich der DSGVO umfasst sind.⁸⁴

Sofern sich jedoch der Firmenwortlaut einer juristischen Person aus den Namen von einer 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.⁸⁵

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 als auch juristische Personen.⁸⁶ Daher richtet sich der grundrechtliche Schutz gem § 1 DSG auch auf juristische Personen, wodurch nach systematischer Interpretation der Begriff „betroffene Personen“ in den einfachgesetzlichen Bestimmungen des DSG auch juristische Personen erfasst.⁸⁷ Juristischen Personen 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.⁸⁸

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) Verantwortlichen

Basierend auf der bisherigen und maßgeblichen Rechtsprechung⁸⁹ des Europäischen Gerichtshofs (EuGH) zur diffizilen Rechtslage hinsichtlich der Qualifikation eines oder mehrerer verantwortlichen datenverarbeitenden Akteure 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.⁹⁰

⁸³ Vgl gem Art 1 Abs 1-3, Art 4 Z 1 sowie ErwGr 14 Satz 1 DSGVO.

⁸⁴ 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.“

⁸⁵ 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.

⁸⁶ 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.

⁸⁷ 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.

⁸⁸ *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).

⁸⁹ 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.

⁹⁰ EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317, Rz 34.

- 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.⁹¹
- Gemeinsame Verantwortlichkeit setzt nicht voraus, dass sämtliche Verantwortliche für dieselbe Verarbeitungstätigkeit einen (gemeinsamen) Zugang zu den betreffenden personenbezogenen Daten haben müssen.⁹²
- 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.⁹³ Daher kann die Verantwortlichkeit bestimmter Verantwortlicher in verschiedenen Phasen und in unterschiedlichem Ausmaß ausgeprägt sein, wodurch der Grad der Verantwortlichkeit variieren kann.⁹⁴ 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, wodurch der einflussausübende Akteur (A) letztendlich an der Entscheidung über die Zwecke und Mittel der Verarbeitung faktisch mitwirkt, woraus die gemeinsame Verantwortlichkeit resultieren kann.⁹⁵
- 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.⁹⁶
- Für die Entscheidung über Zwecke und Mittel der Verarbeitung bedarf es keiner schriftlichen Anleitung oder Anweisung zur gemeinsamen Datenverarbeitung.⁹⁷

⁹¹ EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 36 ff, 39.

⁹² EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 38.

⁹³ EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.

⁹⁴ EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.

⁹⁵ EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 68, 70 ff.

⁹⁶ Vgl. EuGH C-25/17 VbR 2018/110 (202).

⁹⁷ EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 67.

- Eine gemeinsame Entscheidung über das Mittel der Verarbeitung (wie Social Plug-In⁹⁸) kann darin liegen, dass ein *Verantwortlicher* ein solches technisches Verarbeitungsmittel zur Verarbeitung einsetzt, durch das der Anbieter des Mittels an derselben davon umfassten Verarbeitungstätigkeit partizipieren kann.⁹⁹
- 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.¹⁰⁰
- 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.¹⁰¹

4.3.3 Altersnachweis laden und anzeigen

Für die Rollenverteilung bezüglich der Funktion digitaler Altersnachweis, vor allem im Hinblick auf die Rolle des oder der *Verantwortlichen*, kommt dem Begriff der „*rechtlichen Verantwortlichkeit*“¹⁰² maßgebliche Bedeutung zu. Denn dieser Beurteilungsaspekt geht aus Art 4 Z 7, 2. Halbsatz DSGVO hervor und demnach kann der *Verantwortliche* bzw die bestimmten Kriterien für seine Benennung im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden, sofern die Zwecke und Mittel der Verarbeitung durch das jeweilige Recht auch vorgegeben sind. So schlägt sich dieser Beurteilungsaspekt vor allem im öffentlichen Recht nieder, weshalb sowohl einem privaten als auch öffentlich-rechtlichen datenverarbeitenden Akteur kraft nationalem Recht bestimmte Aufgaben, die im öffentlichen Interesse liegen,¹⁰³ oder konkrete Verarbeitungstätigkeiten zugewiesen werden können, woraus sich basierend auf deren expliziter Zuständigkeit hierfür ihre rechtliche Verantwortlichkeit betreffend der mit den zugewiesenen Aufgaben einhergehenden Verarbeitung von personenbezogenen Daten ergeben kann.

In Anbetracht des Beurteilungsaspekts der rechtlichen Verantwortlichkeit sind vor allem die §§ 28 Z 1 iVm 7 Abs 2 iVm 4 Abs 8 iVm 4 Abs 6 EGOvG iVm § 2 BMG einschlägig, welche die Zuständigkeit für die Bereitstellung des digitalen Altersnachweises und sohin die rechtliche Verantwortlichkeit an das Bundesministerium für Finanzen übertragen.¹⁰⁴ Hinsichtlich Ergänzungsregister liegt nach §§ 7 Abs 2 iVm

⁹⁸ Social Plug-Ins können als Mittel der Verarbeitung angesehen werden, da durch deren Einbindung in Websites die Möglichkeit der Verarbeitung (Erhebung oder/und Übermittlung) von personenbezogenen Daten (auch durch Dritte) begründet wird -EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77.

⁹⁹ EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77, 79.

¹⁰⁰ EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 80 ff, 84.

¹⁰¹ EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 74, 85.

¹⁰² *Buder in Jahnel* (Hrsg), *Datenschutzrecht*, 97 (110); *Hartung in Kühling/Buchner*, *DS-GVO/BDSG² Art 4 Nr 7 Rz 15*.

¹⁰³ Vgl *Raschauer in Sydow*, *Europäische Datenschutzgrundverordnung² Art 4 Rz 141*; *Hartung in Kühling/Buchner*, *DS-GVO/BDSG² Art 4 Nr 7 Rz 14*.

¹⁰⁴ Anlage zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriensgesetz 1986 – BMG), BGBl I 1986/76 idF BGBl I 2022/98; siehe erläuternd: <https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehorde> (abgerufen am 23.08.2023). Vor den Arbeiten an diesem Bericht kam es zu einem Übergang der Zuständigkeit für die Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung

28 Z 2 E-GovG ebenfalls eine rechtliche Verantwortlichkeit des BMF vor und bildet eine vom digitalen Nachweis des Alters unabhängige Verarbeitungstätigkeit.

Die Materialien¹⁰⁵ führen erläuternd aus:

“Wie im Allgemeinen Teil der Erläuterungen dargestellt, soll den durch die Bundesministerengesetz Novelle 2017, BGBl. I Nr. 164/2017, erfolgten Veränderungen bei den Zuständigkeiten der jeweiligen Bundesministerinnen oder Bundesministern Rechnung getragen werden, indem die notwendigen legislativen Anpassungen vorgenommen werden.”

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“¹⁰⁶, zumal die vollumfängliche Verantwortung über eine Datenverarbeitung nur jener Akteur trägt, der über die Zwecke und Mittel der Verarbeitung entscheidet.¹⁰⁷ Diesbezüglich ist hervorzuheben, dass das BMF im Rahmen des gesetzlichen Auftrages federführend an der Parametrierung der Funktion beteiligt ist und damit auch wesentlichen faktischen Einfluss auf die Systemausgestaltung nimmt. Das BMF beauftragt den Betrieb der Schnittstelle zwischen Bürger und ID-Austria, weshalb es insgesamt als verantwortliche Stelle zu qualifizieren ist.

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BMF des BRZ als *Auftragsverarbeiter*, welches im Auftrag des BMF die Schnittstelle zwischen ID-Austria (bzw den einschlägigen Registern) und Nutzer*innen betreibt.

Nach § 16 Abs. 1 MeldeG sind die Meldebehörden gemeinsame Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 Abs. 1 DSGVO für das Zentrale Melderegister (ZMR).

Nach § 22b PassG sind die Passbehörden gemeinsame Verantwortliche gemäß Art 4 Z 7 in Verbindung mit Art 26 Abs 1 DSGVO für das Zentrale Identitätsdokumentenregister (IDR). Der Bundesminister für Inneres übt für das Zentrale Melderegister gemäß § 16 Abs. 2a MeldeG und nach § 22b Abs. 1b PassG für das Zentrale Identitätsdokumentenregister die Funktion des Auftragsverarbeiters gemäß Art 4 Z 8 iVm Art 28 Abs 1 DSGVO aus.

Die mit Teilen der Entwicklung beauftragte Younix Identity AG verarbeitet im Rahmen ihrer Entwicklungstätigkeit keine personenbezogenen Daten und hat (auch in Supportfällen) keinen Zugriff auf Daten des Produktivsystems. Ihr fällt daher keine datenschutzrechtliche Rolle zu.

Das BMF hat weder faktischen Einfluss auf den Betrieb des zentralen Melderegisters bzw. des Identitätsdokumentenregisters noch liegt in diesem Zusammenhang eine rechtliche Verantwortlichkeit vor. Zwar greift das BMF auf Daten der Register zu, um diese an Nutzer*innen bereitzustellen, es hat jedoch keinen Einfluss darauf, welche Daten im Register anfallen und wie diese gehalten werden. Eine bloße Zugriffsmöglichkeit sollte keine gemeinsame Verantwortlichkeit begründen.

für das Service und die Interaktion mit Bürgern und Unternehmen und damit der zuständigen Abteilung e-Government Bürger als Teil der Sektion Digitalisierung und e-Government vom BMDW hin zum beim Bundesministerium für Finanzen (BMF) neu eingerichteten Staatssekretariat.

¹⁰⁵ ErläutRV 381 BlgNR 26. GP 2.

¹⁰⁶ Hödl in *Knyrim*, *DatKomm* Art 4 Rz 83.

¹⁰⁷ Hödl in *Knyrim*, *DatKomm* Art 4 Rz 83; *Buder* in *Jahnel* (Hrsg), *Datenschutzrecht*, 97 (101).

Verantwortliche:

- BMF: Betrieb Funktion digitaler Altersnachweis, Betrieb Ergänzungsregister (ErNP)
- Meldebehörden: Zentrales Melderegister
- Passbehörden: Identitätsdokumentenregister (IDR)

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Altersnachweis
- BMI: Betrieb Zentrales Melderegister und Identitätsdokumentenregister

4.3.4 Alter nachweisen

Die Nutzer*in verarbeitet keine Daten der überprüfenden Person (oder sonstige Fremddaten). Die Verarbeitungstätigkeiten der Nutzer*in beschränken sich auf die Verarbeitung eigener Daten weshalb keine datenschutzrechtliche Verantwortlichkeit vorliegt.

Die Verantwortlichkeit für den Betrieb der Funktion ist die ist gleich gelagert wie bei „Ausweis laden und anzeigen“. Siehe: 4.3.3.

Die überprüfende Person verarbeitet im Zuge des Vorweisens Daten der Nutzer*in. Sie hat auch ein Interesse an der Datenverarbeitung, da diese eine Voraussetzung für eine Transaktion oder sonstige Interaktionen mit der Nutzer*in ist. Ob der organisierenden und koordinierenden Tätigkeiten¹⁰⁸ des BMF ist das Vorliegen einer gemeinsamen Verantwortlichkeit zwischen überprüfender Person und BMF zu erwägen. Die überprüfende Person entscheidet jedoch autonom, ob sie einen Prüfungsvorgang startet und verfolgt daneben eigenständige, auf konkrete Beziehungen zur Nutzer*in gerichtete Interessen. Das BMF hat weder unmittelbare noch mittelbare Interessen an den konkreten verarbeiteten Daten oder den Verarbeitungszwecken. Somit liegt auch hier keine gemeinsame Verantwortlichkeit vor.

Verantwortliche:

- BMF: Betrieb Funktion digitaler Altersnachweis
- Überprüfende Person: Überprüfung der Altersstufe sowie des aktuellen Lichtbilds für jeweils eigene Zwecke

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Altersnachweis

4.3.5 Altersnachweis aktualisieren

Die Verantwortlichkeit ist gleich gelagert wie bei „Ausweis laden und anzeigen“. Siehe: 4.3.3.

Verantwortliche:

¹⁰⁸ Vgl. EuGH 10. 7. 2018, C-25/17, *Jehovan todistajat*, Rz 73.

- BMF: Betrieb Funktion digitaler Altersnachweis

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Altersnachweis

4.4 Angaben über Maßnahmen zur Einhaltung der DSGVO

Spezifische Maßnahmen, die zur Einhaltung der DSGVO getroffen wurden, sind ausführlich in der Risikobeurteilung in Kapitel 5.2 jeweils bei den einzelnen Risiken dokumentiert. Die im Folgenden dokumentierten grundsätzlichen Maßnahmen betreffen die Einhaltung bestimmter Datenschutzgrundsätze allgemein.

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.¹⁰⁹ 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.¹¹⁰

Die grundlegenden Maßnahmen, die zur Umsetzung des Grundsatzes der Zweckbindung getroffen wurden, sind daher die Festlegung der Zwecke sowie der für die Erfüllung dieser Zwecke erforderlichen Daten, sodass nur Daten verarbeitet werden, die für die jeweiligen Zwecke erforderlich sind. Dies ist erfolgt und in Abschnitt 3.3 dokumentiert. Dort finden sich auch Begründungen für die Erforderlichkeit, soweit es solcher bedarf.

Kernelemente zur Umsetzung der Zweckbindung bei der Gestaltung des Systems im Sinne des Prinzips des Datenschutzes durch Technikgestaltung (Art 25 DSGVO) sind die Autonomie und die zentrale Rolle der betroffenen Person:

- Die betroffene Person kann frei entscheiden, ob sie den digitalen Altersnachweis oder ausschließlich physische Ausweise nutzt.
- Die Implementierung ermöglicht es, dass zum Zweck des Altersnachweises tatsächlich nur die erforderliche Altersstufe, nicht jedoch identifizierende Daten offengelegt werden, wie dies bei physischen Ausweisen unumgänglich ist.
- Die betroffene Person kann den Altersnachweis anzeigen lassen und kann so einschätzen, ob die darin enthaltenen Daten zweckdienlich sind.
- Bevor die überprüfte Person Daten an die prüfende Person übermittelt, wird ihr angezeigt welche Altersklasse die prüfende Person in Erfahrung bringen möchte. Der Prüfungsprozess kann jederzeit abgebrochen werden.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Nachweis vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten, die überdies direkt zwischen den Endgeräten ohne Einbeziehung eines Servers erfolgt.
- Somit kann die betroffene Person selbst entscheiden, zu welchen Zwecken ihre personenbezogenen Daten im Zusammenhang mit digitalen Ausweisen verwendet werden und ob dies überhaupt der Fall sein soll und kann die maximale Selbstbestimmung und Kontrolle über diese Vorgänge ausüben.

¹⁰⁹ Siehe zudem die primärrechtliche Grundlage in Art 8 Abs 2 EU-Grundrechte-Charta (GRC).

¹¹⁰ *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DSGVO (2018) 37.

Im Folgenden werden einzelne zusätzliche Maßnahmen in Bezug auf die jeweiligen Verarbeitungstätigkeiten beschrieben und zum Teil auch weitere Begründungen der Erforderlichkeit bestimmter Verarbeitungsvorgänge genannt.

Altersnachweis laden und anzeigen

Wie unter 3.3.1 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit, den digitalen Altersnachweis auf das Endgerät der Nutzer*in zu laden.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Verschlüsselte Speicherung sowohl der Daten in der Ausweisplattform als auch der Daten auf dem Endgerät
- Grundsätzlich rein automatisierte Verarbeitung in der Ausweisplattform, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt
- Vor dem Laden des digitalen Altersnachweises ist eine Authentifizierung der jeweiligen Nutzer*in an der Plattform erforderlich, womit einem Zugriff bzw einer potenziell zweckwidrigen Verarbeitung durch andere Personen in diesem Zusammenhang entgegengewirkt wird.
- Reine Offline-Speicherung des digitalen Altersnachweises, womit auch einer potenziell zweckwidrigen, serverseitigen Verarbeitung vorgebeugt wird
- Verschlüsselung der in der eAusweise-App gespeicherten Daten
- Daten, die für die Funktionen der App benötigt werden, werden nur im lokalen App-Speicher verwendet und nicht zu iCloud oder äquivalenten Systemen übertragen.
- Die Protokollierung ist auf das technisch notwendige Minimum beschränkt, insbesondere werden Vorgänge des Vorweises und Überprüfen von Ausweisen im System der Ausweisplattform nicht protokolliert.¹¹¹
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen
- Die betroffene Person kann den Altersnachweis anzeigen lassen und kann so einschätzen, ob die darin enthaltenen Daten zweckdienlich sind.
- Nutzer*innen haben es selbst in der Hand, sich von der eAusweise-App abzumelden und haben volle Kontrolle über den dahinterliegenden Zweck. Dabei werden die in der App gespeicherten Altersnachweisdaten gelöscht.

Alter nachweisen

Wie unter 3.3.2 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit das Vorweisen und Überprüfen der Altersstufe.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Das Vorweisen der Altersstufe findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.
- Verschlüsselte Verbindung der dabei involvierten Endgeräte

¹¹¹ <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

- Nutzer*innen können selbst darüber entscheiden, wem sie ihren digitalen Altersnachweis vorweisen und daher mittelbar auch bis zu einem gewissen Grad, zu welchem Zweck diese Daten durch Dritte verarbeitet werden.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Altersnachweis vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten, die überdies direkt zwischen den Endgeräten ohne Einbeziehung eines Servers erfolgt.
- Bevor die überprüfte Person Daten an die prüfende Person übermittelt, wird ihr angezeigt, welche Altersklasse die prüfende Person in Erfahrung bringen möchte. Der Prüfungsprozess kann jederzeit abgebrochen werden.
- Es werden dabei keine personenbezogenen Daten der *prüfenden* Person verarbeitet. Siehe zur Verarbeitung von Daten der *zu überprüfenden* Person die entsprechenden Ausführungen iZm dem Offline-Vorweisen des Nachweises.

Altersnachweis aktualisieren

- Das letzte Aktualisierungsdatum wird angezeigt, um Nutzer*innen die informierte Entscheidung über eine zweckentsprechende Aktualisierung zu ermöglichen.
- Siehe hierzu ansonsten insb die Ausführungen iZm dem Laden des Altersnachweises

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 diese Zwecke notwendige Maß beschränkt sein.¹¹² 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) umgesetzt werden kann, dann ist eine unverschlüsselte Datenhaltung nicht rechtmäßig. Wenn eine längere Löschfrist das Risiko für die Nutzer*innen erhöht, ist die Frist für jeden Anwendungsfall so kurz wie nötig zu wählen.

Der Grundsatz der Datenminimierung und das Prinzip Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gem Art 25 DSGVO wurde in der Gestaltung des Systems von vornherein berücksichtigt. Dies äußert sich wie folgt:

- Die Implementierung ermöglicht es, dass zum Zweck des Altersnachweises tatsächlich nur die erforderliche Altersstufe, nicht jedoch identifizierende Daten offengelegt werden, wie dies bei physischen Ausweisen unumgänglich ist.

¹¹² Siehe auch ErwGr 39 DSGVO.

- Bereits die Architektur des Systems der Ausweisplattform folgt dem datenschutzrechtlichen Prinzip Data Protection by Design „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ und damit auch dem Grundsatz der Datenminimierung; insbesondere werden die durch die betroffene Person auf eigene Initiative geladenen Nachweisdaten ausschließlich auf dem Endgerät der betroffenen Person gespeichert und das Vorweisen und Überprüfen des Nachweises erfolgt ausschließlich offline, dh ausschließlich auf den beiden verwendeten Endgeräten, und somit ohne dass dieser Vorgang eine Datenverarbeitung außerhalb der beiden verwendeten Endgeräte beinhaltet oder auslöst.
- Die Protokollierung ist hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt.¹¹³
- Daten werden gelöscht, wenn sie für ihren Zweck nicht mehr erforderlich sind; siehe dazu insbesondere auch Abschnitt 4.4.3 unten.
- Daten werden nur verarbeitet bzw übermittelt, soweit dies für den jeweiligen Zweck erforderlich ist.
- Zugriffsrechte bestehen nur im erforderlichen Ausmaß.
- Die Aktualisierung von Ausweisdaten erfolgt niemals automatisch, sondern nur auf Initiative der betroffenen Person, was auch der Systematik des § 4 Abs 6 E-GovG entspricht.

4.4.3 Grundsatz der Speicherbegrenzung

Gem Art 5 Abs 1 lit e DSGVO dürfen personenbezogene Daten nur so lange verarbeitet werden, wie es für die Zweckerreichung erforderlich ist oder eine gesetzliche Verpflichtung zur Aufbewahrung oder Archivierung besteht.

Hierzu ist zunächst festzuhalten, dass Nutzer*innen die Löschung von Daten weitgehend selbst bestimmen, indem sie sich von der eAusweise-App abmelden.¹¹⁴

Sofern die Nutzer*in in der eAusweise-App “dieses Gerät abmelden” auswählt, werden jedenfalls alle entsprechenden Daten, die auf diesem Gerät gespeichert sind, gelöscht. Sofern es sich um das einzige bzw letzte Gerät handelt, das die Nutzer*in im Zusammenhang mit der eAusweise-App verwendet, werden zudem auch alle serverseitig in der entsprechenden Datenbank gespeicherten Daten gelöscht, andernfalls nur jene Daten, die in Bezug auf das jeweilige Gerät in jener Datenbank gespeichert sind.

Im Zuge der Anmeldung vergebene Registrierungstoken werden zudem nach deren einmaliger Nutzung aus der entsprechenden Datenbank gelöscht.

4.5 Angaben über die Berücksichtigung der Betroffenenrechte

4.5.1 Gewährleistung der Transparenz und Informationspflichten

Die DSGVO schreibt in Art 12 ff vor, dass der für die Datenverarbeitung *Verantwortliche* den Betroffenen alle nach Maßgabe des Gesetzes erforderlichen Informationen, die sich auf die Verarbeitung be-

¹¹³ <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

¹¹⁴ <https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf> (abgerufen am 24.08.2023).

ziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie außerdem in einer klaren und einfachen Sprache zu übermitteln hat. Dabei geht es für die Betroffenen insb um transparente Information, Kommunikation und entsprechende Modalitäten zur Ausübung ihrer Rechte.

Um dies zu gewährleisten, wird den Betroffenen im Zuge des Registrierungsprozesses zusätzlich zu den zu akzeptierenden Nutzungsbedingungen die Datenschutzerklärung präsentiert. Diese kann auch danach jederzeit in der App im Bereich „Mein Profil“ abgerufen werden.

Außerdem steht den Nutzer*innen im Zusammenhang mit der jedenfalls im Zuge des Registrierungsprozesses einmalig durchzuführenden Identitätsbestätigung der Zugriff auf die Datenschutzerklärung der dafür benötigten ID Austria mittels Link¹¹⁵ offen.

4.5.2 Recht auf Auskunft und Datenübertragbarkeit

Die Betroffenen 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 sowohl in der Datenschutzerklärung als auch auf der entsprechenden Webseite des BMF¹¹⁶ angegeben.

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 Datenschutzerklärung wird auf diesen Anspruch hingewiesen, ebenfalls sind darin die notwendigen Kontaktmöglichkeiten angegeben.¹¹⁷

4.5.3 Recht auf Berichtigung und Löschung

Gem Art 16 DSGVO haben Betroffene das Recht, vom *Verantwortlichen* die unverzügliche Berichtigung sie betreffender personenbezogener Daten zu verlangen, sofern diese unrichtig sein sollten. Dies beinhaltet auch den Anspruch, eine Vervollständigung unvollständiger personenbezogener Daten mittels einer ergänzenden Erklärung zu verlangen. Die für die Wahrnehmung dieses Rechts erforderlichen Kontaktmöglichkeiten sind in der Datenschutzerklärung als auch auf der entsprechenden Webseite des BMF¹¹⁸ angegeben.

Ebenfalls kommt Betroffenen unter den in Art 17 DSGVO beschriebenen Voraussetzungen das Recht zu, vom *Verantwortlichen* die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Voraussetzungen sehen ein Lösungsrecht insbesondere bei unrechtmäßiger Verarbeitung sowie in solchen Fällen vor, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Für die Wahrnehmung dieses Rechts sind sowohl in der Datenschutzerklärung als auch auf der entsprechenden Webseite des BMF¹¹⁹ die erforderlichen Kontaktmöglichkeiten angegeben.

¹¹⁵ Zum Zeitpunkt der Erstellung des Berichts unter <https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html> (abgerufen am 24.08.2023)..

¹¹⁶ Siehe <https://www.bmf.gv.at/public/datenschutz.html> (abgerufen am 24.08.2023).

¹¹⁷ Siehe <https://www.bmf.gv.at/public/datenschutz.html> (abgerufen am 24.08.2023).

¹¹⁸ Siehe <https://www.bmf.gv.at/public/datenschutz.html> (abgerufen am 24.08.2023).

¹¹⁹ Siehe <https://www.bmf.gv.at/public/datenschutz.html> (abgerufen am 24.08.2023).

4.5.4 Rechte auf Einschränkung und Widerspruch

Den Betroffenen steht grundsätzlich das Recht auf Einschränkung der Verarbeitung gem Art 18 DSGVO sowie für jene Fälle der Datenverarbeitung, die auf Art 6 Abs 1 lit e leg cit basieren, das Widerspruchsrecht gem Art 21 leg cit unter den jeweils in diesen Bestimmungen normierten Bedingungen zu. Für die Wahrnehmung dieser Rechte sind sowohl in der Datenschutzerklärung¹²⁰ als auch auf der entsprechenden Website des BMF¹²¹ die erforderlichen Kontaktmöglichkeiten angegeben.

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 Datenschutzerklärung zu finden.¹²²

¹²⁰ Siehe <https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html> (abgerufen am 24.08.2023).

¹²¹ Siehe <https://www.bmf.gv.at/public/datenschutz.html> (abgerufen am 24.08.2023).

¹²² Die zuständige Aufsichtsbehörde ist die Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at, Web: <https://www.dsb.gv.at> (abgerufen am 24.08.2023).

4.6 Datenübermittlung in Drittländer (oder an internationale Organisationen)

Bei keiner der Verarbeitungstätigkeiten, die Gegenstand der vorliegenden DSFA sind, kommt es zu einer Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen.

4.7 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 des Datenschutzbeauftragten zu folgen ist, wird in der Literatur uneinheitlich kommentiert: *Trieb* geht bspw davon aus, dass die DSGVO keine solche Pflicht statuiert;¹²³ *Jandt* sieht in der Bestimmung wiederum eine Pflicht, die Vorschrift treffe jedoch keine Aussage darüber, ob dem Rat des Datenschutzbeauftragten auch zu folgen ist und sehe für diesen auch kein Vetorecht oder Ähnliches vor.¹²⁴ 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.¹²⁵

Der Datenschutzbeauftragte des BMF (Dr. Lang) wurde ab Februar 2023 in die Festlegung der weiteren Vorgehensweise betreffend datenschutzrechtliche Aspekte im Zusammenhang mit der Weiterentwicklung der Ausweisplattform sowie der App eAusweise eingebunden und wurde unter anderem auch im Rahmen der Durchführung dieser Datenschutz-Folgeabschätzung konsultiert.

Ferner ist vom Verantwortlichen gemäß Art 35 Abs 9 DSGVO im Zuge einer DSFA gegebenenfalls der Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen.¹²⁶ Die Bestimmung des Abs 9 schafft grundsätzlich die Möglichkeit, die individuelle Meinung einzelner Betroffener in Erfahrung zu bringen.¹²⁷ Alternativ können auch deren „Vertreter“ herangezogen werden, wobei in erster Linie an verschiedene Interessensvertretungen, Betriebsräte oder Verbraucherschutzverbände 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.¹²⁸ Auch diese Regelung lässt in mehrfacher Hinsicht Deutungsspielräume offen.¹²⁹ Unklarheiten bestehen bspw hinsichtlich des Stellenwerts des Standpunkts für die Einbeziehung in den Prüfprozess der DSFA. Die Formulierung „gegebenenfalls“ lässt auch offen, unter welchen Umständen der Standpunkt einzuholen ist und wann darauf verzichtet werden kann.¹³⁰ Eine bedingungslose Verpflichtung für Verantwortliche zur Einholung wird auf Basis dieser Bestimmung

¹²³ Vgl *Trieb*, in *Knyrim*, DatKomm Art 35 Rz 124.

¹²⁴ Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 18.

¹²⁵ So die *Art-29-Datenschutzgruppe*, WP 243 rev. 01, 17 unter Hinweis auf Art 24 Abs 1 DSGVO.

¹²⁶ Siehe hierzu auch *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgeabschätzung (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.

¹²⁷ Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.

¹²⁸ Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 134; vgl hierzu auch *Martin/Friedewald/Schiering/Mester/Hallinan/Jensen*, Datenschutz-Folgeabschätzung nach Art 35 DSGVO, Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe (2020) 38 ff.

¹²⁹ Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.

¹³⁰ 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.

nicht unterstellt werden können;¹³¹ die jeweilige Vorgehensweise ist jedoch zu dokumentieren bzw zu begründen.¹³²

Zur Fertigstellung der Datenschutz-Folgenabschätzung betreffend digitalen Führerschein und zur Ausweisplattform Phase 1 fanden im Q3/2022 Termine zu fachlichem Austausch mit Vertretern der Zivilgesellschaft und der Forschung statt. Der Austausch soll im Zuge der Vorstellung neuer Funktionen und Updates weiterhin aktiv gepflegt werden.

Dem staatlichen Handeln im Zusammenhang mit dem Betrieb der Ausweisplattform und der Funktionen liegt nichts weniger als das Legalitätsprinzip des Art 18 B-VG zugrunde. Dementsprechend steht das relevante Verwaltungshandeln der parlamentarischen Kontrolle und damit den Vertretern des Volkes. Diese Kontrollmöglichkeit wird auch regelmäßig im Rahmen von parlamentarischen Anfragen hinsichtlich Ausweisplattform ausgeübt (siehe etwa PA 13625/J).

¹³¹ Vgl *Trieb* in *Knyrim*, *DatKomm* Art 35 Rz 131.

¹³² Vgl *Jandt*, in *Kühling/Buchner* *DS-GVO/BDSG* Art 35 Rz 58.

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,¹³³ 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.¹³⁴ 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.¹³⁵ 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.

¹³³ Vgl Jandt, in Kühling/Buchner DS-GVO/BDSG Art 35 Rz 42. Siehe weiterführend auch die Gewährleistungsziele der DSGVO: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Interventionsbarkeit, Nichtverkettbarkeit und Transparenz in Martin et al, Datenschutz-Folgenabschätzung (2020) 55 ff. Vgl auch SDM 11 ff.

¹³⁴ Vgl Martin et al, Datenschutz-Folgenabschätzung 38; vgl European Data Protection Supervisor (EDPS), Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 8.

¹³⁵ Vgl ErwGr 75 DSGVO. Siehe auch Martin et al, Datenschutz-Folgenabschätzung 39 f; zur methodischen Konkretisierung der Begriff “Eintrittswahrscheinlichkeit” und “Schwere” siehe Kapitel 5.1.

Weitere exemplarisch angeführte Bedrohungsszenarien für den Bereich der IT-Sicherheit können ua den IT-Grundschutz-Katalogen des deutschen Bundesamts für Sicherheit in der Informationstechnik entnommen werden.¹³⁶

Unter Bezugnahme auf die vorgenommene Abgrenzung des Gegenstandes der vorliegenden DSFA (siehe in Kapitel 3) ist darauf hinzuweisen, dass im Folgenden nur eine Beurteilung möglicher Risiken im Verantwortungsbereich des BMF vorgenommen werden kann. Insbesondere sind Risiken in der Sphäre jener Verantwortlichen, denen die betroffenen Personen digitale Ausweise vorweisen, weder in der datenschutzrechtlichen Verantwortlichkeit des BMF noch durch das BMF vorhersehbar.

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 der Ausweisplattform 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.¹³⁷

¹³⁶ https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf (abgerufen am 24.08.2023).

¹³⁷ Vgl. *European Data Protection Supervisor (EDPS), Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation* (2019) 6.

5.1 Methodik

Die Methodik der nachfolgenden Risikobeurteilung stützt sich im Kern auf die Risk Management ISO-Norm 31000:2018.¹³⁸ Darüber hinaus wurde Anleihe am Risk Assessment-Leitfaden des deutschen Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom),¹³⁹ sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Fraunhofer-Institutes für System- und Innovationsforschung genommen.¹⁴⁰

Der European Data Protection Supervisor (EDPS) sieht grundsätzlich 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.¹⁴¹

Die Artikel-29-Datenschutzgruppe empfiehlt für die Durchführung einer Risikobeurteilung, mit Verweis auf Art 35 Abs 7 sowie ErwGr 84 und 90 der DSGVO, insb¹⁴²

- 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.¹⁴³

In ErwGr 83 der DSGVO 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.¹⁴⁴

In den methodischen Ausführungen des Fraunhofer-Instituts werden für die generelle Erfassung eines Risikoszenarios wiederum die folgenden übergeordneten Fragen aufgeworfen:¹⁴⁵

- 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 Akteure bzw (nicht-menschliche) Risikoquellen sind dabei wie involviert?

¹³⁸ <https://www.iso.org/standard/65694.html> (abgerufen am 24.08.2023).

¹³⁹ Vgl Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung, <https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf> (abgerufen am 24.08.2023).

¹⁴⁰ Vgl Martin et al, Datenschutz-Folgenabschätzung 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.

¹⁴¹ Vgl European Data Protection Supervisor (EDPS), Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 6.

¹⁴² 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.

¹⁴³ Siehe Art 35 Abs 7 lit d sowie ErwGr 84 und 90 DSGVO.

¹⁴⁴ Vgl ErwGr 83 DSGVO.

¹⁴⁵ Vgl Martin et al, Datenschutz-Folgenabschätzung 43.

- Welche Abhilfemaßnahmen sind bereits implementiert bzw geplant?¹⁴⁶

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:¹⁴⁷

- **Risikoidentifikation** (Beschreibung des Szenarios, Ermittlung beteiligter Akteure und betroffener Personen, Bestimmung der Ursache und Ermittlung der Risikoquelle als Auslöser, 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 und neuerliche Risikobewertung)

Zum Prozess der Beurteilung wird in ErwGr 76 DSGVO 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*“.¹⁴⁸

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

¹⁴⁶ Zudem kann ergänzt werden, welche zusätzlichen Maßnahmen sich bestimmen lassen um die identifizierten Risiken zu mitigieren.

¹⁴⁷ 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 38 ff.

¹⁴⁸ Vgl ErwGr 76 DSGVO.

Risikobeurteilung (Template)

1) Risikoidentifikation	Risikobeschreibung
	Beschreibung und kurze deskriptive Erläuterung des Szenarios, Nennung beteiligter Akteure und Personen, ¹⁴⁹ Nennung verarbeiteter Datenkategorien
	Risikoquelle
	<p>Was sind die auslösenden Elemente für den Schadenseintritt?</p> <p>Handelt es sich um eine menschliche oder technische Risikoquelle?</p> <p>Interne menschliche Quellen:</p> <p>Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar</p> <p>Externe menschliche Quellen:</p> <p>Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Angreifer oder Verursacher außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Systems oder der Betroffenen</p> <p>Interne / externe technische Quellen:</p> <p>Systemfehler (Software/Hardware) führen zu Verlust, Veränderung; Nichtverfügbarkeit oder missbräuchlicher Verwendung personenbezogener Daten</p> <p>Bsp Risikoquelle:</p> <ul style="list-style-type: none"> • Interne Mitarbeiter*innen, • Externe Mitarbeiter*innen, • Betroffene, • Sonstige Dritte, • Softwarefehler, • Hardwaredefekt (physikalisch), • Umwelteinflüsse (Naturgewalt), • Cyberkriminelle (Hacker/Schadsoftware), • staatliche Institutionen (Nachrichtendienste, Strafverfolgung), • Geschäftsführung.
	Risikoursache
<p>Was löst den Eintritt des Schadens aus und führt zur „Verwirklichung des Risikos“?</p> <p>Dies dürfte regelmäßig in der Nichteinhaltung der Datenschutzgrundsätze (Art 5 Abs 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art 12 bis 22 DSGVO) oder</p>	

¹⁴⁹ Siehe hierzu auch die Auflistung an zu prüfenden Organisationen bei *Friedewald/Bieker/Obersteller/Nebel/Martin/Rost/Hansen* Datenschutz-Folgenabschätzung (2017), https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf (abgerufen am 24.08.2023) 30 f.

	<p>anderer Verstöße gegen die DSGVO (wie zB einem ungerechtfertigten Datentransfer ins Ausland) liegen.¹⁵⁰</p> <p>Bsp Ursachen:</p> <ul style="list-style-type: none"> • 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 den Zweckbindungsgrundsatz.
	<p>Möglicher Schaden für die betroffenen Personen</p>
	<p>Welche Schäden und Beeinträchtigungen von Rechten und Freiheiten der Betroffenen lassen sich feststellen? Handelt es sich um einen physischen, materiellen oder immateriellen Schaden?¹⁵¹</p> <p>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)</p> <p>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</p> <p>Bsp immaterielle Schäden: gesellschaftliche und soziale Nachteile (wie etwa Rufschädigung oder Verleumdung, Mobbing, Diskriminierung usw); Schädigung der Privatsphäre (wie etwa 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)</p>

¹⁵⁰ Siehe hierzu auch *Martin et al*, Datenschutz-Folgenabschätzung 38 ff.

¹⁵¹ *Friedewald et al*, Datenschutz-Folgenabschätzung 30 f.

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

3) Maßnahmen	Bestehende Maßnahmen
	Nennung bestehender technischer und organisatorischer Abhilfemaßnahmen •

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

Der Prozess der datenschutzrechtlichen Risikobeurteilung erfolgt im vorliegenden Fall somit anhand der folgenden fünf Teilschritte: Risikoidentifikation; Risikoanalyse und -bewertung; Ermittlung bestehender Maßnahmen und Festlegung zusätzlicher Maßnahmen der Risikomitigierung und schließlich die neuerliche Risikoanalyse und -bewertung unter Berücksichtigung der zum Zeitpunkt der Beurteilung tatsächlich vorgesehenen Abhilfemaßnahmen. Die zuvor dargelegte Sachverhaltsbeschreibung dient als Informationsgrundlage der Risikobeurteilung.¹⁵² Die Risikoidentifikation bezieht sich auf diese Grundlage und extrahiert daraus für die weitere Risikoanalyse wesentliche datenschutzrechtliche Aspekte wie die Nennung der involvierten Akteure bzw Personen, die Beschreibung der Risikoursache bzw -quelle, sowie die Bestimmung möglicher physischer, materieller oder immaterieller Schäden.

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.¹⁵³ Im Zuge der Risikobeurteilung sind

¹⁵² Vgl *Martin et al*, Datenschutz-Folgenabschätzung 38 ff.

¹⁵³ Die Benennung der Merkmalsausprägung variiert; bei *Martin et al*, Datenschutz-Folgenabschätzung 47 ist bspw von „geringfügig“, „überschaubar“, „substantiell“ und „groß“ die Rede; siehe weiterführend auch *Friedewald et al*, Datenschutz-Folgenabschätzung 31 f; vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 29; vgl CNIL, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.

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 erui- ren.¹⁵⁴ Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annah- men zur angemessenen Einstufung des identifizierten Risikoszenarios.¹⁵⁵

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit¹⁵⁶

Wert	Beschreibung
Vernachlässigbar	Es erscheint nicht sehr wahrscheinlich, dass eine Bedrohung eintritt (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweisleseger-ät und einen Zugangscode gesichert ist).
Eingeschränkt	Es erscheint schwierig, dass eine Bedrohung eintritt (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
Wesentlich	Es erscheint möglich, dass eine Bedrohung eintritt (zum Beispiel: Diebstahl von Pa-pierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
Maximal	Es erscheint einfach, dass eine Bedrohung eintritt (zum Beispiel: Diebstahl von Pa-pierdokumenten aus einer öffentlich zugänglichen Lobby).

Tabelle 2: Risikoausprägungen für Schadensausmaß¹⁵⁷

Wert	Beschreibung
Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Prob-lemem 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 ernsthaf-ten Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequ-zen, die sie nicht überwinden können.

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in einer Risikomatrix verortet. Der Risikograd ist methodisch definiert als das Produkt von Eintrittswahrscheinlichkeit und Schadensaus- maß.¹⁵⁸ 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,¹⁵⁹ wie in der nachfolgenden Risi- komatrix dargestellt.

¹⁵⁴ Vgl. ErwGr 75 und 76 DSGVO.

¹⁵⁵ Vgl. *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 ff; vgl. *CNIL*, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.

¹⁵⁶ Vgl. *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 30 f.

¹⁵⁷ Vgl. *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 f.

¹⁵⁸ Vgl. *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 8 (9).

¹⁵⁹ Vgl. *Martin et al*, Datenschutz-Folgenabschätzung 46; vgl. hierzu weiterführend auch *Friedewald et al*, Datenschutz-Fol- genabschätzung 31.

Tabelle 3: Risikomatrix

		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)

Um der grundrechtlichen Schutzkonzeption des Datenschutzrechts gerecht zu werden, wird im Schrifttum jedoch auch empfohlen, dass die Beurteilung eines Risikos nicht ausschließlich anhand der quantitativen Matrix von Schadenshöhen (Schwere) und Eintrittswahrscheinlichkeiten bestimmt werden sollte. 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.¹⁶⁰

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.¹⁶¹ Dabei werden bestehende technische und organisatorische Maßnahmen zur Behandlung 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 Technikgestaltung (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) Genüge zu tun.¹⁶²

Die in Art 35 Abs 7 lit d DSGVO genannte „Bewältigung“ wird gemeinhin auch als „Reduktion“ bzw „Eindämmung“ verstanden.¹⁶³ Durch die Maßnahmen sollten zumindest alle als „hoch“ bewerteten Risiken so weit reduziert werden, dass sie nur noch als „normal“ einzustufen sind.¹⁶⁴ Dabei ist es nicht zwangsläufig notwendig, zusätzliche Maßnahmen zu implementieren; mitunter kann es auch sinnvoller sein, bestehende Maßnahmen zu stärken.¹⁶⁵

¹⁶⁰ Vgl *Friedewald et al*, Datenschutz-Folgenabschätzung 31.

¹⁶¹ Siehe Art 35 Abs 7 lit d DSGVO; vgl *Martin et al*, Datenschutz-Folgenabschätzung 38.

¹⁶² Vgl ErwGr 78 DSGVO.

¹⁶³ Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46.

¹⁶⁴ Vgl *Martin et al*, Datenschutz-Folgenabschätzung 47.

¹⁶⁵ Vgl *Martin et al*, Datenschutz-Folgenabschätzung 48.

In Art 32 Abs 1 DSGVO werden zur Gewährleistung eines angemessenen Schutzniveaus folgende Optionen bzw Maßnahmen der Risikobehandlung angeführt:¹⁶⁶

- 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 DSGVO auf Maßnahmen der Zugriffsbeschränkung bzw Zugangskontrollen verwiesen.¹⁶⁷ Die verschiedenen Maßnahmen, Garantien und Verfahren sollen letztlich den Schutz personenbezogener Daten sicherstellen und die Einhaltung der Bestimmungen dieser Verordnung nachweisen.¹⁶⁸

Nach Ermittlung und Bestimmung der Maßnahmen wird im vorliegenden Modell der Risikobeurteilung der Schritt zur Risikoanalyse und -bewertung wiederholt und eine neuerliche Klassifizierung und Errechnung des Risikograds vorgenommen. Über diesen zweiten Analyse- bzw Bewertungsschritt wird der potenzielle 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*.¹⁶⁹ Dabei kommt vor allem eine weitere Minimierung des Risikos in Frage, in dem in der weiteren künftigen Entwicklung des Systems zusätzliche Maßnahmen umgesetzt werden, die entweder den Schaden oder die Eintrittswahrscheinlichkeit verringern. Zudem kann auch eine gänzliche Eliminierung des Risikos erfolgen, indem die in Rede stehende Datenverarbeitung komplett vermieden wird.¹⁷⁰ 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.¹⁷¹

¹⁶⁶ Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 33 f.

¹⁶⁷ Für eine Liste typischer Abhilfemaßnahmen siehe die weiterführenden Angaben bei *Martin et al*, Datenschutz-Folgenabschätzung 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.

¹⁶⁸ Vgl ErwGr 90 DSGVO.

¹⁶⁹ In der IT- und Datensicherheit wird nicht davon ausgegangen, dass absolute Sicherheit erreicht werden kann. Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 46; siehe hierzu weiterführend *Rothmann*, Der Fehler im Feld der Überwachung, in *Winter/Schausberger* (Hrsg) Parapraxis (2016) 65 ff.

¹⁷⁰ 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.

¹⁷¹ Vgl *Trieb* in *Knyrim*, DatKomm, Art 35 Rz 112.

5.2 Risikobeurteilung

Auf Basis des vorgestellten methodischen Modells erfolgt die eigentliche Umsetzung der Risikobeurteilung. Die Risikobewertung gilt als Kern bzw Herzstück der DSFA.¹⁷² Dabei ist zu beachten, dass konsequent die Perspektive der Betroffenen eingenommen wird. Die Folgen- und Risikoabschätzung ist als Prozess zu verstehen und laufend an die tatsächlichen Gegebenheiten und Entwicklungen anzupassen und zu aktualisieren.

Anzumerken ist, dass die Risiken, die mit ID Austria verbunden sind, bereits in der gesondert durchgeführten Datenschutz-Folgenabschätzung zu ID Austria behandelt wurden. Diese Risiken können aufgrund der Anbindung der eAusweise-App bzw Ausweisplattform an ID Austria mittelbar auch hier relevant sein. Soweit sich durch diese Anbindung keine Besonderheiten ergeben, werden diese Risiken im Folgenden nicht mehr gesondert behandelt.

5.2.1 Unfreiwillige Nutzung des digitalen Altersnachweises

1) Risikoidentifikation	Risikobeschreibung
	Die betroffene Person möchte zwar den digitalen Altersnachweis nicht nutzen, installiert und verwendet diesen aber dennoch, weil sie entweder durch äußere Umstände einem Druck ausgesetzt ist, diese zu nutzen, oder der (irrigen) Annahme unterliegt, künftig beim Bezug bestimmter Leistungen (zB Einlass ins Gastgewerbe) in digitaler Form vorweisen zu müssen. Insbesondere falls die Nutzung des digitalen Altersnachweises künftig weite Verbreitung finden sollte, kann es zu Formen sozialen Drucks oder faktischen Zwangs zur Nutzung des digitalen Altersnachweises als Nachweis des Alters anstelle eines physischen Ausweises kommen. Dies unter der Annahme, dass sich der Auslesevorgang für die überprüfende Person unter Umständen einfacher gestaltet und weiters angesichts der Tatsache, dass die Fälschungssicherheit höher ist. So könnte es beim digitalen Altersnachweis der prüfenden Person (bei Nutzung eigener spezifischer Applikationen) leichter fallen Daten automatisiert zu verarbeiten und Querverbindungen zwischen Nachweisen anzustellen als es bisher beim physischen Ausweis der Fall war. Sollte sich dies manifestieren, würde dies eine Zunahme der Verarbeitung personenbezogener Daten und Intensivierung des damit in Verbindung stehenden Grundrechtseingriffs bedeuten.
	Risikoquelle
	Interne / Externe menschliche Quellen: <ul style="list-style-type: none"> • Entscheidungsträger*innen des <i>Verantwortlichen</i> • Interne Mitarbeiter*innen • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache

¹⁷² Vgl *Trieb* in *Knyrim*, *DatKomm* Art 35 Rz 113.

	<ul style="list-style-type: none"> • Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu entsprechendem Druck zur Nutzung der Ausweis-Apps • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer ungewollten bzw unrechtmäßigen Datenverarbeitung. • Einschränkung der informationellen Selbstbestimmung • Unpräzise oder fehlende Kommunikation durch den <i>Verantwortlichen</i> oder andere zuständige Stellen, dass analoge Ausweise weiterhin uneingeschränkt genutzt werden kann • Größere Zahl von Privaten, insbesondere Unternehmen, deren Verhalten zu entsprechenden Drucksituationen führt und welche Nachweisdaten mit Applikationen erheben welche über den Funktionsumfang der eAusweise-App hinausgehen. • Politische Entscheidungen und/oder die fortschreitende Verwaltungsdigitalisierung könnten zu einem faktischen Zwang zur Verwendung der eAusweise-App führen, falls ohne diese bestimmte Verwaltungsprozesse unverhältnismäßig erschwert oder gar nicht mehr möglich sind.
	Möglicher Schaden für die betroffenen Personen
	<p>Immaterielle Schäden:</p> <ul style="list-style-type: none"> • Verarbeitung personenbezogener Daten gegen den Willen der betroffenen Person • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer unrechtmäßigen Datenverarbeitung. • Unfreiwillige oder auch bloß unreflektierte Herausgabe der Identität oder einzelner Attribute, weil diese bei bestimmten Diensten nunmehr verlangt werden, da die eAusweise-App deren komfortable Herausgabe ermöglicht • Verringerte Anonymität und verstärktes Hinterlassen personenbezogener Datenspuren im Alltagsleben • Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung der eAusweise-App bzw des digitalen Altersnachweises verbunden sind, da die betroffene Person diese eigentlich gar nicht verwenden würde, wenn sie sich frei entscheiden hätte können

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2) Kommentar: Risiko manifestiert sicher erst bei Nutzung	Eingeschränkt (2) Kommentar: Das bloße Alter ist in keine Voraus-	Normal (4)

	proprietärer Applikationen auch Püfer*innen	setzung zum Bezug essentieller Leistungen, weshalb kein Auftreten schwerwiegender Drucksituationen denkbar erscheint.	
--	---	---	--

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Stringente Außenkommunikation hinsichtlich Nutzungsmöglichkeiten des physischen Altersnachweises • Das Datenschutzrecht untersagt das Verlangen bestimmter Attribute, wenn dies für den jeweiligen Zweck nicht erforderlich ist (insb Art 5 Abs 1 DSGVO, Grundsatz der Rechtmäßigkeit, Grundsatz der Zweckbindung und Grundsatz der Datenminimierung). • Weder existiert nach aktueller Gesetzeslage irgendein Anwendungsfall, der die Verwendung eines digitalen Nachweises oder derzeit konkret des digitalen Altersnachweises als einzig zulässige Variante für die Bürger*in festlegt, noch ist nach derzeitigem Wissensstand ein solcher angedacht oder gar in Planung. In der Außenkommunikation wird das BMF deutlich auf diesen Umstand hinweisen. • Aufgrund der Datensparsamen Konzeption und Implementierung des Altersnachweises, insbesondere durch Übermittlung der Altersklassen und nicht des Geburtsdatums als datensparsame Alternative zum physischen Ausweis, wird dieses Risiko weitgehend entschärft. Dies betrifft vor allem auch den Aspekt einer möglichen personenbezogenen Weiterverarbeitung der Daten, da Daten zur Herstellung des Personenbezugs nicht von der Übermittlung umfasst sind. • <i>Geplante</i> Maßnahme: Implementierung der Steuerung der Auslesbarkeits- bzw Überprüfungsmöglichkeiten durch Key Attestation Mechanisms

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Vernachlässigbar (1)	Eingeschränkt (2)	Gering (2)

5.2.2 Diskriminierung aufgrund von Nicht-Nutzung des digitalen Altersnachweises

1) Risikoidentifikation	Risikobeschreibung
	<p>Die betroffene Person verwendet den Altersnachweis bewusst nicht, wobei dies verschiedene Gründe haben kann, zB mangelnde digitale Affinität, Mangel eines Smartphones mit Biometrie-Funktion, Ablehnung der eAusweise-App und/oder der ID Austria, Ablehnung der Nutzung der Biometrie-Funktion des Smartphones, insbesondere aus Datenschutzgründen etc, und erleidet dadurch Nachteile. Durch die potenziell weitverbreitete Verwendung des Systems und etwa des digitalen Altersnachweises könnte es uU zu Situationen kommen, in denen insb private <i>Verantwortliche</i> auf das Vorweisen eines digitalen Nachweises bestehen, insb weil im Vergleich dazu das Auslesen für die überprüfende Person leichter und die Fälschungssicherheit höher ist. Dadurch würden potenziell Personen diskriminiert, die den digitalen Altersnachweis bewusst nicht verwenden oder nicht die entsprechend vorausgesetzte digitale Infrastruktur bzw auch etwa eine ID Austria haben (wollen oder können).</p>
	Risikoquelle
	<p>Interne / Externe menschliche Quellen:</p> <ul style="list-style-type: none"> • Entscheidungsträger*innen des <i>Verantwortlichen</i> • Interne Mitarbeiter*innen • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache
	<ul style="list-style-type: none"> • Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu weitverbreiteter Nutzung der eAusweise-App bzw des digitalen Altersnachweises • Einschränkung der informationellen Selbstbestimmung • Verhalten privater Anbieter (zB Gastgewerbe), das zu entsprechenden Situationen führt • Politische Entscheidungen und/oder die fortschreitende Verwaltungsdigitalisierung könnten zu einer Diskriminierung bei Nicht-Nutzung der eAusweise-App führen, falls künftig ohne diese bestimmte Verwaltungsprozesse erschwert oder gar nicht mehr möglich sind. • Unpräzise oder fehlende Kommunikation durch den <i>Verantwortlichen</i> oder andere zuständige Stellen, dass der physische Ausweise weiterhin uneingeschränkt genutzt werden kann
Möglicher Schaden für die betroffenen Personen	
<p>Materielle Schäden:</p> <ul style="list-style-type: none"> • Möglicher Ausschluss von system- oder alltagsrelevanten Diensten, womit auch finanzielle Schäden verbunden sein könnten (zB höherer Warenpreis soweit ein niedrigerer Warenpreis digitalen Altersnachweis voraussetzt) 	

	Immaterielle Schäden: <ul style="list-style-type: none"> • Einschränkungen in Teilen der (zB privaten) Lebensführung • Einschränkungen in der Nutzung von Diensten aufgrund der Ablehnung, die eAusweise-App bzw den digitalen Altersnachweis zu nutzen
--	--

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Das bloße Alter ist in keine Voraussetzung zum Bezug essentieller Leistungen, weshalb kein Auftreten schwerwiegender Drucksituationen denkbar erscheint.	Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Verwendung von physischen Ausweisen weiterhin möglich. • Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Altersnachweises als moderne Inklusionsvariante eine erleichterte und datensparsame Variante und somit gleichsam als Gegenteil eines Diskriminierungsinstruments konzipiert ist

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (1)	Eingeschränkt (2) Kommentar: Das bloße Alter ist keine Voraussetzung zum Bezug essentieller Leistungen, weshalb kein Auftreten schwerwiegender Drucksituationen denkbar erscheint.	Gering (2)

5.2.3 Unbefugter Zugriff auf IDR/ZMR/ERnP über das AWP-Backend

1) Risikoidentifikation	Risikobeschreibung
	Eine unbefugte Person verschafft sich über das AWP-Backend Zugriff auf eines der dahinterliegenden Register. Über das AWP-Backend ist der Bezug von Daten aus dem IDR/ZMR/ERnP (über die ID-Austria) möglich, um Daten der jeweiligen Nutzer*innen beziehen zu können. Zumal es sich dabei um hochqualitative Daten handelt, könnte ein Interesse daran bestehen, unbefugter Weise darauf zuzugreifen und entsprechende Daten (§ 22b Abs 1 und Abs 4 iVm § 22a Abs 1 Passgesetz 1992 iVm § 18 Abs 1 E-GovG.) anderer Personen zu akquirieren.
	Risikoquelle
	Interne /Externe menschliche Quellen:
	<ul style="list-style-type: none"> • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware)
	Interne / externe technische Quellen:
	<ul style="list-style-type: none"> • Softwarefehler
	Risikoursache
<ul style="list-style-type: none"> • Unbefugte bzw unrechtmäßige Verarbeitung der in IDR/ZMR/ERnP enthaltenen Daten 	
Möglicher Schaden für die betroffenen Personen	
Immaterielle Schäden	
<ul style="list-style-type: none"> • wirtschaftliche oder gesellschaftliche Nachteile durch Bekanntgabe der Wohnadresse (Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte) • gesellschaftliche Nachteile 	

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Keine ein-griffsintensiven Datenkategorien in fraglichen Registern enthalten	Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
--------------	-----------------------------

	<ul style="list-style-type: none"> • Über das AWP-Backend besteht kein direkter Zugriff auf IDR/ZMR/ERnP. Die Daten werden standardmäßig über die ID Austria ausgeliefert. • Die Schnittstelle zur ID-Austria durch die AWP benötigt zwingend das verschlüsselte bPK der jeweiligen Bürger*in.
--	--

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Eingeschränkt (2)	Normal (4)

5.2.4 Protokollierung zu vieler personenbezogener Daten

1) Risikoidentifikation	Risikobeschreibung		
	<p>Risiko, dass im Zuge der Verwendung der eAusweise-App auf der Ebene des IDR/ZMR/ERnP mehr personenbezogene Daten protokolliert werden, als dies zur Erfüllung der Anforderungen des Datenschutzrechts und zur Erfüllung aller anderen legitimen Anforderungen unbedingt erforderlich ist. Damit ist stets das Risiko verbunden, dass diese Protokolldaten offengelegt bzw zweckwidrig verarbeitet werden und deshalb bekannt wird, an welchen Stellen Betroffene ihren digitalen Nachweis verwendet haben.</p>		
	Risikoquelle		
	<p>Interne technische Quellen:</p> <ul style="list-style-type: none"> • Softwarearchitektur, welche etwa standardmäßig bestimmte Daten protokolliert • Softwarekonfiguration 		
	Risikoursache		
	<ul style="list-style-type: none"> • Das System ist so gestaltet bzw konfiguriert, dass mehr personenbezogene Daten protokolliert werden, als zur Erfüllung legitimer Anforderungen unbedingt erforderlich ist. • Softwarebetriebsbedingte Protokollierungsanforderungen können dem Grundsatz der Datenminimierung entgegenstehen. 		
	Möglicher Schaden für die betroffenen Personen		
<p>Materielle Schäden</p> <ul style="list-style-type: none"> • Diskriminierung (zB bei Vertragsabschlüssen), berufliche Nachteile <p>Immaterielle Schäden</p> <ul style="list-style-type: none"> • 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)	Wesentlich (3) Kommentar: Keine besonders eingriffsintensiven Datenkategorien betroffen.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen	
	<ul style="list-style-type: none"> • Privacy by Design: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. • Die Protokollierung unterliegt klaren gesetzlichen Regeln. 	

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2) Kommentar: Protokollierung nur während des Ladens von Aus- oder Nachweisen.	Eingeschränkt (2) Kommentar: Die Protokollierung ist auf das technisch notwendige Minimum beschränkt; entsprechend reduziert ist auch das mit Protokolldaten verbundene potenzielle Schadensausmaß.	Normal (4)

5.2.5 Missbräuchliche Verwendung von Protokolldaten

1) Risikoidentifikation	Risikobeschreibung
	Risiko, dass Protokolldaten auf der Ebene des IDR/ZMR/ERnP offengelegt bzw zweckwidrig verarbeitet werden und deshalb insbesondere bekannt wird, an welchen Stellen Betroffene ihren digitalen Nachweis verwendet haben.
	Risikoquelle
	Interne/externe menschliche Quellen: <ul style="list-style-type: none"> • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) • staatliche Institutionen (Nachrichtendienste, Strafverfolgung) Interne / externe technische Quellen: <ul style="list-style-type: none"> • Softwarefehler (zB mangelhafte Verschlüsselung, offene Schnittstellen)
	Risikoursache
	<ul style="list-style-type: none"> • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben

	<ul style="list-style-type: none"> • Unbefugte Offenlegung von und Zugang zu Daten • Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten • Verwendung der Daten durch die Verantwortlichen zu inkompatiblen Zwecken • Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler) • Verarbeitung über die Speicherfrist hinaus • Verarbeitung entgegen dem Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	<p>Materielle Schäden</p> <ul style="list-style-type: none"> • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust <p>Immaterielle Schäden</p> <ul style="list-style-type: none"> • Rufschädigung • Verletzung der Privatsphäre • 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; ebenso unbefugter Zugriff von außen durch einen Angriff	Wesentlich (3) Kommentar: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen	
	<ul style="list-style-type: none"> • Privacy by Design: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. 	

	<ul style="list-style-type: none"> • Privacy by Design: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. • Die Protokollierung unterliegt klaren gesetzlichen Regeln.
--	--

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Eingeschränkt (2) Kommentar: Die Protokollierung ist auf das technisch notwendige Minimum beschränkt; entsprechend reduziert ist auch das mit Protokolldaten verbundene potenzielle Schadensausmaß.	Normal (4)

5.2.6 Nichtverfügbarkeit des Systems

1) Risikoidentifikation	Risikobeschreibung
	<p>Das System steht der Nutzer*in nicht zur Verfügung und sie kann daher ihren digitalen Nachweis nicht vorweisen.</p> <p>Das System ist auf das reibungslose Zusammenspiel durch von verschiedenen Akteuren verwaltete Systemkomponenten angewiesen, weshalb die Verfügbarkeit eher eingeschränkt sein kann als beim physischen Ausweis. Soweit kein (physisches) Substitut mitgeführt wird, könnten sich in Einzelfällen unter Umständen verwaltungsrechtliche Folgen oder Folgen oder Nachteile im Rechtsverkehr ergeben.</p>
	Risikoquelle
	<p>Interne / Externe menschliche Quellen:</p> <ul style="list-style-type: none"> • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Betroffene • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) <p>Interne / externe technische Quellen:</p> <ul style="list-style-type: none"> • Softwarefehler • Endgerät • Hardwaredefekt (physikalisch) <p>Sonstige Quellen:</p> <ul style="list-style-type: none"> • Umwelteinflüsse (Naturgewalt)
	Risikoursache
	<p>Der Eintritt des Risikos wird zunächst durch das Vertrauen der Nutzer*innen auf die Datenverfügbarkeit ermöglicht, soweit sie in diesem Vertrauen davon absehen physische Ausweise mitzuführen.</p> <p>Das Risiko kann eintreten durch eine Fehlfunktion im Authentifizierungsvorgang, sodass der an sich Berechtigte 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 z.B. verursacht werden durch:</p> <ul style="list-style-type: none"> • Fehlfunktion in der Biometrie-Komponente des Smartphones (dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemherstellern) • Die Biometriekomponente steht bei einer ganzen Gerätegeneration nicht mehr zur Verfügung, weil sie aufgrund einer dokumentierten Kompromittierung deaktiviert werden musste (dies liegt außerhalb der

	<p>Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemherstellern).</p> <ul style="list-style-type: none"> • Geringfügig geänderte physische Merkmale der Nutzer*in, durch Verletzungen, Hautprobleme etc <p>Neben dieser spezifischen Ursache kann das Verfügbarkeitsrisiko auch durch viele verschiedene andere Ursachen (insb Komponenten der ID Austria, Ausweisplattform, Register, Endgeräte) ausgelöst werden. Zu beachten sind vor allem Systemteile, die vielleicht nicht als kritisch wahrgenommen werden, deren Ausfall aber trotzdem zur Nichtverfügbarkeit des Gesamtsystems führen kann.</p>
	Möglicher Schaden für die betroffenen Personen
	<p>Materielle Schäden:</p> <ul style="list-style-type: none"> • Materielle Schäden sind vorstellbar, zB wenn Nutzer*innen rasch eine kostenverursachende Alternative in Anspruch nehmen müssen, zB durch Zusatzgebühren für manuelle/analoge Prozesse bei Dienstleistungsunternehmen <p>Immaterielle Schäden:</p> <ul style="list-style-type: none"> • wirtschaftliche oder gesellschaftliche Nachteile • Verweigerung des Zugangs oder Einlasses, weil sich die betroffene Person nicht ausweisen kann

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	<p>Maximal (4)</p> <p>Kommentar: Bei entsprechender Verbreitung sind durch Endgeräte bedingte Risikoeintritte sehr wahrscheinlich.</p>	<p>Eingeschränkt (2)</p> <p>Kommentar: Der Zugang zu Leistungen oder der Einlass kann (temporär) verwehrt sein.</p>	<p>Normal (8)</p>

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Physische Ausweise können weiterhin diskriminierungsfrei in allen Lebenslagen verwendet werden. Unterstützung bzw Dokumentation (zB FAQ) bzgl Hinterlegung neuer biometrischer Daten am Endgerät. • Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Altersnachweises als moderne Inklusionsvariante und somit gleichsam als Gegenteil eines Einschränkungsinstruments konzipiert ist. • Das Vorweisen und Prüfen des Altersnachweises läuft offline ab und ist nicht von der Verfügbarkeit von Serverarchitektur abhängig.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Eingeschränkt (2)	Normal (6)

5.2.7 Vorweisen eines gefälschten digitalen Altersnachweises

1) Risikoidentifikation	Risikobeschreibung		
	<p>Es gelingt einem Angreifer, manipulierte Nachweisdaten (eine falsche Altersstufe) via Bluetooth zu übermitteln, sodass die Überprüfungs-Funktion die Manipulation nicht erkennt und die Überprüfung des manipulierten Nachweises erfolgreich verläuft.</p> <p>Alternativ präsentiert der Angreifer gefälschte Ausweisdaten (zB als bearbeiteten Screenshot) und überzeugt die prüfende Person es bei einer Sichtprüfung zu belassen und keine Übermittlung der Altersstufen anzufordern.</p>		
	Risikoquelle		
	<p>Externe menschliche Quelle:</p> <ul style="list-style-type: none"> • Sonstige Dritte 		
	Risikoursache		
	<p>Die Ursache kann eine Schwachstelle in der Funktion zur Erzeugung (insbesondere Signieren) und Übermittlung der Ausweisdaten via Bluetooth oder eine Schwachstelle in der Funktion zur Überprüfung der via Bluetooth empfangenen Ausweisdaten (insbesondere Signaturprüfung) sein.</p> <p>Daneben kann die Ursache in mangelndem Verständnis der prüfenden Person über die Funktion des Altersnachweises sein, was sie dazu veranlasst, die Sichtprüfung zu akzeptieren.</p>		
	Möglicher Schaden für die betroffenen Personen		
<p>Materielle Schäden</p> <ul style="list-style-type: none"> • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust <p>Immaterielle Schäden</p> <ul style="list-style-type: none"> • wirtschaftliche oder gesellschaftliche Nachteile 			

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Maximal (4)	<p>Wesentlich (3)</p> <p>Kommentar: Aufgrund der Unterbreitung einer falschen Altersklasse sind keine schwerwiegenden Schäden zu erwarten.</p>	Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Es sind folgende Basismaßnahmen im Einsatz, die dem entgegenwirken: <ul style="list-style-type: none"> ○ Die Ausweisdaten sind signiert und beim Überprüfen findet eine Signaturprüfung statt. Eine erfolgreiche Fälschung der Ausweisdaten wäre nur unter der Annahme der Korruption der verwendeten Public Key Infrastructure des Systems der AWP denkbar, einschließlich der dazu erforderlichen Überwindung mannigfaltiger Sicherheitsmaßnahmen. ○ Beim Herzeigen der Ausweisdaten muss der Besitzer nachweisen, dass er im Besitz des privaten Schlüssels ist, dessen öffentlicher Teil im Nachweis eingebunden ist. Dies bedeutet, dass die signierten Ausweisdaten alleine nicht für den Identitätsnachweis reichen, es muss auch der Beweis erbracht werden, dass man im Besitz des Schlüssels ist, der mit dem Nachweis verknüpft wird. ○ Manuelle Prüfung des Lichtbildes durch prüfende Person. ○ Hinweis, dass Sichtprüfung der Applikation der überprüften Person keine hinreichende Grundlage für Vertrauen in den Nachweis bildet

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Wesentlich (3)	Normal (6)

5.2.8 Vorweisen einer faktisch unrichtigen Altersstufe

1) Risikoidentifikation	Risikobeschreibung
	Die prüfende Person führt nach dem faktischen Erreichen einer neuen Altersstufe keine Aktualisierung des Altersnachweises durch. Wenn nun geprüft wird, ob die faktisch schon überschrittene Altersstufe noch nicht erreicht wurde (also etwa ob Alter < 16 Jahre) wird als Prüfergebnis angezeigt, dass dies zutrifft, obwohl dies faktisch nicht mehr der Fall ist.
	Risikoquelle
	Externe menschliche Quelle:
	<ul style="list-style-type: none"> • Sonstige Dritte
	Risikoursache
	Überprüfte Person aktualisiert Altersstufen nicht obwohl sie faktisch eine neue Altersstufe erreicht hat.
	Möglicher Schaden für die betroffenen Personen
Materielle Schäden	
<ul style="list-style-type: none"> • Übervorteilung (zB bei Vertragsabschlüssen) (die überprüfende Person betreffend) • finanzieller Verlust (die überprüfende Person betreffend) 	
Immaterielle Schäden	
<ul style="list-style-type: none"> • gesellschaftliche Nachteile • Verarbeitung unrichtiger Daten 	

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Gefahren für die betroffene Person würden in erster Linie davon ausgehen, dass sie sich als älter ausgeben kann, als sie ist. Das ist hier nicht der Fall. Wenn sich eine Person als jünger ausgibt, als sie ist, sind keine besonders schwerwiegenden Schäden zu erwarten.	Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Der überprüfenden Person wird der Zeitpunkt der letzten Aktualisierung angezeigt • Hinweis in Applikation, dass die Zuverlässigkeit der Daten hinsichtlich Altersstufe im Zusammenhang mit der letzten Aktualisierung stehen • Gültigkeit der Altersstufen ist technisch begrenzt auf 1 Jahr

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Vernachlässigbar (1) Kommentar: Prüfende Person kann Aktualisierung anfordern und Schaden leicht überwinden	Gering (2)

5.2.9 Vorweisen des Nachweises einer anderen Person

1) Risikoidentifikation	Risikobeschreibung
	<p>Ein Angreifer verwendet den eAusweise-App-Login einer anderen Person auf deren Endgerät oder einem anderen Endgerät, um einen - an sich nicht manipulierten - Nachweis dieser anderen Person vorzuweisen. Dies kann entweder mit Einverständnis der anderen Person oder gegen deren Willen erfolgen. Dem Angreifer gelingt es, sich als diese andere Person auszugeben, weil die überprüfende Person anhand des übermittelten Lichtbildes nicht erkennt, dass die Person auf dem Lichtbild nicht diejenige ist, die den Nachweis vorweist.</p> <p>Anzumerken ist: Zu einer Risikoerhöhung kommt es aufgrund des digitalen Altersnachweises (z.B. gegenüber dem physischen Führerschein) nur durch die (theoretische) Möglichkeit der Verwendung des eAusweise-App-Logins gegen den Willen der betroffenen Person, sodass der Angreifer nichts physisch entwenden muss. Die Problematik der Überprüfung des Gegenübers auf Übereinstimmung mit dem vorgewiesenen Foto besteht hingegen auch bei physischen Ausweisen und die Qualität der Fotowiedergabe in der App eAusweise wird demgegenüber deutlich höher sein.</p>
	Risikoquelle
	<p>Externe menschliche Quellen:</p> <ul style="list-style-type: none"> • Sonstige Dritte
	Risikoursache
	<ul style="list-style-type: none"> • Bewusster, zielgerichteter Angriff • Schwachstelle in der ID Austria-Authentifizierung • Mangelnde Kontrolle über die Systeme der Smartphone-Hersteller und Betriebssystem-Hersteller • Strukturelle Probleme der Biometrie • Veraltete Gerätegenerationen: Viele Android- und Apple-Geräte (ab iOS 15), 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 Reparatur geben, etc) • Bewusste Weitergabe der elektronischen Identität durch den Betroffenen an den Angreifer
	Möglicher Schaden für die betroffenen Personen
<p>Materielle Schäden</p> <ul style="list-style-type: none"> • Diskriminierung (zB bei Vertragsabschlüssen) 	

	<ul style="list-style-type: none"> • berufliche Nachteile • finanzieller Verlust <p>Immaterielle Schäden</p> <ul style="list-style-type: none"> • Identitätsdiebstahl oder -betrug • Psychologische Schäden • Rufschädigung • Verletzung der Privatsphäre • wirtschaftliche oder gesellschaftliche Nachteile
--	--

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3) Kommentar: Das Gegenüber kann und sollte das Foto kontrollieren; diesbzgl keine Risikoerhöhung gegenüber physischem Ausweis, bei dem dasselbe Problem besteht	Wesentlich (3) Kommentar: Aufgrund der Unterbreitung einer falschen Altersklasse sind keine schwerwiegenden Schäden zu erwarten.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Biometrische Authentifizierung beim Öffnen der eAusweise-App; dadurch wird das Vorweisen eines fremden digitalen Nachweises verglichen mit einem physischen Ausweis deutlich erschwert; dies ist auch gegen die bewusste Weitergabe durch rechtmäßige Ausweisinhaber*innen wirksam. • Der digitale Altersnachweis führt somit aufgrund der implementierten Sicherheitsmaßnahmen im Vergleich zur analogen Variante tatsächlich zu einer Reduzierung des Risikos des Vorweisens eines fremden Nachweises.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	-Wesentlich (3)	Normal (6)

5.2.10 Rechtswidrige Verarbeitung durch Zugriffsbefugte

1) Risikoidentifikation	Risikobeschreibung
	Der <i>Verantwortliche</i> , ein <i>Auftragsverarbeiter</i> oder eine eigenmächtig handelnde, zugriffsberechtigte Person verarbeitet personenbezogene Daten in zweck- bzw rechtswidriger Weise weiter.
	Risikoquelle
	Interne / Externe menschliche Risikoquellen: <ul style="list-style-type: none"> • Interne Mitarbeiter*innen • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) Interne technische Risikoquellen: <ul style="list-style-type: none"> • Softwarearchitektur
	Risikoursache
	<ul style="list-style-type: none"> • Unbefugte oder unrechtmäßige Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten zB durch einen <i>Verantwortlichen</i> an anderen beteiligten <i>Verantwortlichen</i>, dem Zugang nicht zustünde • Verwendung der Daten durch die Verantwortlichen zu inkompatiblen Zwecken/Verarbeitung wider den Zweckbindungsgrundsatz (etwa zur Ausforschung von Personen)
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: <ul style="list-style-type: none"> • 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 Immaterielle Schäden: <ul style="list-style-type: none"> • Es kann zu einer ungerechtfertigten Beeinträchtigung von Rechten der Betroffenen kommen. • 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
	Wesentlich (3)	Wesentlich (3) Kommentar: Der rechtswidrige Zugriff und die zweckwidrige Verarbeitung können für die Betroffenen zu wesentlichen Schäden führen.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Zuweisung von Rollen durch gesetzliche Bestimmungen bzw <i>Auftragsverarbeitervereinbarungen</i> • Schulungen von Mitarbeiter*innen im Hinblick auf Umgang mit Personenbezogenen Daten • Klare Kommunikation und Aufklärung über Konsequenzen • Protokollierung und Kontrolle von Zugriffen interner Mitarbeiter*innen auf Daten • Technische Ausgestaltung iSd Minimierung von Zugriffsmöglichkeiten • Der Betrieb erfolgt gemäß den Vorgaben des BMF für den Betrieb von eGovernment-Infrastruktur.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Wesentlich (3)	Normal (6)

5.2.11 Auslesen des Nachweises ohne Rechtsgrundlage

1) Risikoidentifikation	Risikobeschreibung
	<p>Der Überprüfende hat keine Rechtsgrundlage, die Daten der betroffenen Person zu verarbeiten (was das Überprüfen des Nachweises miteinschließt) und er dürfte daher von der betroffenen Person das Vorweisen eines Nachweises nicht verlangen. Zwar wird es stets zulässig sein, dass die betroffene Person ihren Nachweis freiwillig vorweist und dieser in der Folge auch durch die überprüfende Person gelesen wird, aber es ist sehr leicht möglich, dass diese Freiwilligkeit eingeschränkt ist (Drucksituation, Erforderlichkeit zum Erhalt einer Leistung, Aussicht auf eine Gegenleistung oÄ).</p> <p>Eine Risikoerhöhung durch den digitalen Nachweis des Alters gegenüber einem physischen Ausweis ist nicht gegeben.</p>
	Risikoquelle
	<p>Externe menschliche Quellen:</p> <ul style="list-style-type: none"> • Sonstige Dritte • Cyberkriminelle
	Risikoursache
	<ul style="list-style-type: none"> • Bewusster, zielgerichteter Angriff • Druck auf die betroffene Person • Leichtgläubigkeit der betroffenen Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit digitalen Aus- oder Nachweisen • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Unbefugte Offenlegung von und Zugang zu Daten • Verarbeitung entgegen den Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	<p>Materielle Schäden</p> <ul style="list-style-type: none"> • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust <p>Immaterielle Schäden</p> <ul style="list-style-type: none"> • Rufschädigung • gesellschaftliche Nachteile • Verletzung der Privatsphäre

	<ul style="list-style-type: none"> • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte
--	---

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Maximal (4)	Eingeschränkt (2) Kommentar: Übermittelte Daten weisen geringe Eingriffsintensivität auf	Normal (8)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Die betroffene Person muss beim Auslesen stets involviert sein. Insofern besteht keine Risikoerhöhung gegenüber einem physischen Ausweis. (Wie oben beschrieben bedeutet das aber nicht, dass stets Freiwilligkeit vorliegt.)

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Maximal (4)	Vernachlässigbar (1) Kommentar: Keine Risikoerhöhung ggü physischem Ausweis	Normal (4)

5.2.12 Intransparenz der Datenverarbeitung

1) Risikoidentifikation	Risikobeschreibung		
	Besonders angesichts der Komplexität des Systems ist es denkbar, dass das datenschutzrechtliche Prinzip der Transparenz nicht vollständig gewährleistet wird und es deshalb zu einer nicht nachvollziehbaren, unklaren Datenverarbeitung kommt. Allenfalls kommt der <i>Verantwortliche</i> den Informationspflichten zwar nach, die betroffene Person ist aufgrund der technischen und funktionalen Komplexität jedoch uU nicht in der Lage, die Auswirkungen der Datenverarbeitung auf ihre Rechte und Freiheiten angemessen zu beurteilen.		
	Risikoquelle		
	Interne menschliche Risikoquelle:		
	<ul style="list-style-type: none"> • Entscheidungsträger*innen des <i>Verantwortlichen</i> • Interne Mitarbeiter*innen 		
	Interne technische Risikoquelle:		
	<ul style="list-style-type: none"> • Systemkomplexität 		
Risikoursache			
<ul style="list-style-type: none"> • Unzureichende Informationserteilung • Unzureichende Informationsaufnahme durch die betroffene Person 			
Möglicher Schaden für die betroffenen Personen			
Immaterielle Schäden			
<ul style="list-style-type: none"> • Verlust der Kontrolle über die Verarbeitung der eigenen personenbezogenen Daten • Erschwerung der Rechtsausübung • 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
	Wesentlich (3)	Wesentlich (3)	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Es wird eine Datenschutzerklärung in einfacher und klarer Sprache bereitgestellt.¹⁷³ • Das System wird über die Website oesterreich.gv.at via FAQs zu Sicherheit und Datenschutz grundlegend erklärt. • Es wird eine Datenschutz-Folgenabschätzung durchgeführt und der Bericht darüber wird der Öffentlichkeit zur Verfügung gestellt.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Wesentlich (3)	Normal (6)

¹⁷³ Die Datenschutzerklärung kann in der entsprechenden Applikation abgerufen werden.

5.2.13 Nutzung der Ökosysteme von Google und Apple

1) Risikoidentifikation	Risikobeschreibung
	<p>Einzig für die Zugänglichmachung sowie die weitere Verwendung der eAusweise-App wird die technische Infrastruktur US-amerikanischer IT-Konzerne genutzt; dies bedeutet jedoch nicht, dass die Ausweisdaten selbst an diese Konzerne kommuniziert werden. Mangels alternativer Möglichkeiten begibt sich die österreichische Verwaltung damit in ein Abhängigkeitsverhältnis, allerdings ebenfalls nur in jenem Ausmaß, wie das bereits bei der ID Austria erfolgte. Diese Abhängigkeit 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 US-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 zweck- bzw rechtswidrigen Datenverarbeitung 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. Zudem besteht das Risiko des Zugriffs auf diese Daten durch US-Sicherheitsbehörden.¹⁷⁴ Dem kann entgegengehalten werden, dass sich die betroffenen Personen bereits auf dieser Infrastruktur befinden und sich selbst dorthin begeben hätten, aber der Staat steht hier in einer besonderen Verantwortung und kann durch seine Systeme auch bewirken, dass sich noch mehr Menschen dorthin begeben, um diese Systeme verwenden zu können.</p>
	Risikoquelle
	<p>Interne / Externe menschliche und strukturelle Quelle:</p> <ul style="list-style-type: none"> • Entscheidungsträger*innen des <i>Verantwortlichen</i> • Externe Entscheidungsträger*innen
	Risikoursache
	<ul style="list-style-type: none"> • Management-Entscheidung auf Seiten des <i>Verantwortlichen</i> zur Nutzung der Infrastruktur von Google und Apple als Plattformprovider für die Distribution der eAusweise-App. Man sieht sich aus Sicht des <i>Verantwortlichen</i> dazu gezwungen, auf die Plattformen und Technologien Dritter zurückzugreifen, um digitale Ausweise für weite Teile der Bevölkerung möglichst einfach verfügbar zu machen bzw die Nutzung zu fördern. Eine entsprechende Verpflichtung ist auch im Vorschlag COM(2023) 127 final der Europäischen Kommission zur Novellierung der europäischen Führerscheinrichtlinie enthalten. • Verarbeitung entgegen den Datenschutzgrundsätzen (Art 5 DSGVO) durch die Verflechtung einer staatlichen E-Government-Anwendung mit

	<p>börsennotierten US-amerikanischen IT-Konzernen, da keine eigene Distributionsplattform ohne Weiterverarbeitung der Nutzer*innendaten zu Werbezwecken verwendet wird</p> <ul style="list-style-type: none"> • Datenverarbeitung wird nicht auf das notwendige Maß beschränkt; insuffiziente Umsetzung des Grundsatzes der Datenminimierung • Verarbeitung von personenbezogenen Daten zu inkompatiblen Zwecken (wie 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
	<p>Immaterielle Schäden:</p> <ul style="list-style-type: none"> • 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
	<p>Maximal (4) Kommentar: Das Risiko ist bereits eingetreten.</p>	Wesentlich (3)	Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	<ul style="list-style-type: none"> • Physische Ausweise können weiterhin diskriminierungsfrei in allen Lebenslagen verwendet werden. • Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Daten, die für die Funktionen der App benötigt werden, werden nur im lokalen App-Speicher verwendet und nicht zu iCloud oder äquivalenten Systemen übertragen.

	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
--	------------------------------------	-----------------------	------------------------

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Wesentlich (3) Kommentar: Wie in den angeführten Maßnahmen ersichtlich, bestehen Alternativen.	Wesentlich (3)	Normal (9)
---	---	----------------	------------

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 – nach derzeitigem Stand keine als hoch zu bewertenden Risiken bestehen.

Aufgrund des Tempos der technologischen Veränderung 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.¹⁷⁵

Sollte aus dieser Beurteilung künftig hervorgehen, dass Verarbeitungsvorgänge ein hohes Risiko bergen, wird der *Verantwortliche* geeignete Maßnahmen anstreben, um diese einzudämmen. Sollte der *Verantwortliche* im Rahmen der verfügbaren Technik und angemessener Implementierungskosten nicht in der Lage sein, diese Risiken einzudämmen, ist gem Art 36 DSGVO die Datenschutzbehörde zu konsultieren.¹⁷⁶

Ebenfalls gilt es – neben den hier geprüften und analysierten Risiken – gesamtgesellschaftliche Entwicklungen 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 digitale Ausweise aus verschiedenen Gründen nicht verwenden möchten oder können.

¹⁷⁵ Siehe Art 5 Abs 2 sowie Art 35 Abs 11 DSGVO.

¹⁷⁶ Siehe ErwGr 84 DSGVO; vgl *Martin et al*, Datenschutz-Folgenabschätzung 49.

6 Fazit und getroffene Entscheidungen

Im Ergebnis zeigt die vorliegende DSFA, dass die identifizierten verbleibenden Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der gesetzten Maßnahmen des *Verantwortlichen* nicht als hoch einzustufen sind. Aus derzeitiger Sicht besteht somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Art 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.

6.1 Zusammenfassung der Ergebnisse

Zusammenfassend kann festgehalten werden, dass

- personenbezogene Daten nur von berechtigten Stellen verarbeitet bzw übermittelt werden;
- nur die für die Zweckerfüllung erforderlichen Daten verarbeitet werden;
- personenbezogene Daten einem stringenten Löschkonzept unterliegen;
- gespeicherte personenbezogene Daten strengen Zugriffsbeschränkungen unterliegen;
- der Grundsatz der Datenminimierung und das Prinzip „Privacy by Design“ insbesondere durch das Vorweisen der bloßen Altersstufe sowie durch die Implementierung des Vorweisens als Vorgang, der vollständig offline, ohne die Beteiligung eines Servers stattfindet, bereits in der grundlegenden Gestaltung des Systems berücksichtigt wurden;

Der DSFA-Bericht gelangt somit zu dem Ergebnis, dass eine Vielzahl von Garantien und Maßnahmen bestehen, welche die Risiken der geplanten Verarbeitungsprozesse eindämmen, den Schutz personenbezogener Daten sicherstellen sowie die Einhaltung aller datenschutzrechtlichen Anforderungen gewährleisten. Dies wird durch den vorliegenden Bericht dokumentiert.

6.2 Pflicht zur künftigen Überprüfung

Der *Verantwortliche* hat gem Art 35 Abs 11 DSGVO künftig Überprüfungen durchzuführen, ob die Verarbeitung gemäß der vorliegenden Datenschutz-Folgenabschätzung durchgeführt wird und ob hinsichtlich der mit den gegenständlichen Verarbeitungsvorgängen verbundenen Risiken Änderungen eingetreten sind, und diese gegebenenfalls neu zu bewerten.

Eine derartige Neubewertung kann sich insb durch Änderungen am gegenständlichen System, durch technische Entwicklungen aber auch durch normative Änderungen der einschlägigen Rechtsvorschriften oder durch Gerichtsentscheidungen ergeben und im Ergebnis dazu führen, dass andere oder zusätzliche Abhilfemaßnahmen für eine datenschutzkonforme Verarbeitung vorzunehmen sind.¹⁷⁷

¹⁷⁷ Vgl Jandt in Kühling/Buchner, DS-GVO/BDSG Art 35 Abs 11 Rz 59 ff.

Glossar und Abkürzungsverzeichnis

ABl:	Amtsblatt der Europäischen Union („L“ steht in diesem Zusammenhang für Rechtsakte, „C“ für Mitteilungen und Bekanntmachungen und „S“ für Ausschreibungen) ¹⁷⁸
Abs:	Absatz
AES 256-Bit-Verschlüsselung:	Advanced Encryption Standard (Chiffre) mit Schlüssellänge von 256 Bit
Anm:	Anmerkung
Art:	Artikel
A-SIT:	Zentrum für sichere Informationstechnologie - Austria
AWP:	Ausweisplattform
BfDI:	Bundesbeauftragter für den Datenschutz und die Informationssicherheit (Deutschland); Bundesbehörde
BGBI:	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
BlgNR:	Beilagen zu den stenographischen Protokollen des Nationalrates ¹⁷⁹
BMDW:	Bundesminister für Digitalisierung und Wirtschaftsstandort
BMF	Bundesministerium für Finanzen
BMG:	Bundesministeriengesetz 1986 BGBI I 1986/76

¹⁷⁸ Siehe *Dax/Hopf*, Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europäische Rechtsquellen⁸ (2019) 43.

¹⁷⁹ *Dax/Hopf*, AZR⁸ 43.

BMI:	Bundesminister für Inneres
BMK:	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
bPK:	bereichsspezifische Personenkennzeichen; dieses dient grundsätzlich der eindeutigen Identifikation von natürlichen Personen in einem konkreten Verwaltungsverfahren ¹⁸⁰ 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, indem anstelle der Bereichskennung die Stammzahl oder das bPK des <i>Verantwortlichen</i> des privaten Bereichs verwendet wird (§ 14 Abs 1 E-GovG).
BRZ:	Bundesrechenzentrum GmbH
BSI:	Bundesamt für Sicherheit in der Informationstechnik; deutsche Bundesbehörde
bsph:	beispielhaft
bspw:	beispielsweise
B-VG:	Bundes-Verfassungsgesetz BGBl I 1930/1
bzgl:	bezüglich
bzw:	beziehungsweise

¹⁸⁰ Vgl. Feik/Randl in Jahnel/Mader/Staudegger (Hrsg), IT-Recht³ (2012), 399.

Client-Komponente:	Entweder Digitales-Amt-App, Third-Party-App oder Mobiler Web-Browser, die/der Signaturerstellungs-Requests erstellt, übermittelt und empfängt
CNIL:	französische Datenschutzbehörde
CRL:	Certificate Revocation List; Widerrufsliste (von Zertifikaten)
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 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABI L 2016/119, 1
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, ABI L 1995/281, 31
E-GovG:	E-Government-Gesetz; Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, BGBl I 2004/10
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, ABi L 2014/257, 73

eIDAS 2-VO (Vorschlag):

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM(2021) 281 final 2021/0136(COD)

E-ID:

elektronischer Identitätsnachweis (s insb § 2 Z 10 E-GOVG)

E-ID-Inhaber:

E-ID-Nutzer*in nach erfolgreichem Registrierungsprozess

ErläutRV:

Erläuterungen zur Regierungsvorlage

ErwGr:

Erwägungsgrund

EuGH:

Europäischer Gerichtshof

f/ff:

folgende(r/s)/folgende

FAQ:

Frequently Asked Questions

FSG:

Führerscheingesetz BGBl I 1997/120

FSR:

Führerscheinregister

gem:

Gemäß

ggf:

gegebenenfalls

grds:

grundsätzlich

HSM:

Hardware Security Module

iaR:

in aller Regel

idF:

in der Fassung

IDP:

Identity Provider

idR:

in der Regel

IMEI:

International Mobile Equipment Identity; eindeutige Nummer des Endgeräts

IMSI:	International Mobile Subscriber Identity; eindeutige Nummer des Netzteilnehmers
insb:	insbesondere
iSd:	im Sinne der/des
iSe:	im Sinne einer/eines
ISMS:	Information Security Management System
ISO/IEC 18004:	ISO-Standard: Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification
ISO/IEC 18013-5:	ISO-Standard: Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application
iSv:	im Sinne von
iVm:	in Verbindung mit
iZm:	im Zusammenhang mit
leg cit:	legis citatae, der zitierten Norm
lit:	litera/literae
krit:	Kritisch
MDS:	Minimaldatensatz (bzw Minimal Dataset)
MSISDN:	Mobile Station Integrated Services Digital Network – weltweit eindeutige Mobilfunk-Rufnummer
mwN	mit weiteren Nachweisen
Nr:	Nummer
oÄ:	oder Ähnliches
OIDC:	Open ID Connect
Personenbindung:	Dadurch wird dem E-ID-Inhaber von der SZRB elektronisch signiert oder besiegelt bestätigt, dass ihm ein oder mehrere bereichsspezifische Personenkenneichen zugeordnet sind. Die Per-

	sonenbindung wird dabei mit dem Minimal Dataset (bestehend aus Vor- und Nachnamen sowie Geburtsdatum) verbunden, wodurch die SZRB auch die Richtigkeit der Zuordnung bestätigt.
Pkt:	Punkt
Portal Austria:	Das Portal Austria ist ein zentrales Access Management Portal im Bundesrechenzentrum für den sicheren Zugang zu Webanwendungen der Verwaltung.
Portalverbund:	Der Portalverbund ermöglicht den Zugriff auf behördenübergreifende Webanwendungen und die Verwaltung der zugehörigen Rechte. ¹⁸¹
PVP:	Portalverbundprotokoll; wird ua dazu verwendet, um auf das SPRS zuzugreifen
Rn:	Randnummer
Rsp:	Rechtsprechung
Rz:	Randziffer
S:	Satz
SAML 2.0:	Security Assertion Markup Language 2.0
Secure Element:	dedizierte, separate, manipulationssichere Hardware zum Speichern kryptografischer Daten am Endgerät (Android Keystore bzw Secure Enclave (Apple))
SLA:	Service Level Agreement
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.
sog:	sogenannte(n/r/s)

¹⁸¹ <https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund>. (abgerufen am 24.08.2023).

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
Stammzahl:	eine Zahl, die einem Betroffenen zu dessen eindeutiger Identifikation zugeordnet ist, welche auch für die Ableitung von bereichsspezifischen Personenkennzeichen bestimmt ist ¹⁸²
SZRB:	Stammzahlenregisterbehörde; nunmehr im Wirkungsbereich des BMF ¹⁸³
tlw:	teilweise
TOM(s):	(geeignete) technische und organisatorische Maßnahmen gem DSGVO ¹⁸⁴
ua:	unter anderem
UDID:	Unique Device Identifier; eindeutige Geräte- nummer für Apple-Produkte
uE:	unseres Erachtens
usw:	und so weiter
uU:	unter Umständen
vbPK-VT:	verschlüsseltes bereichsspezifisches Personen- kennzeichen des Bereichs Verkehr und Technik
vbPK-ZP	verschlüsseltes bereichsspezifisches Personen- kennzeichen des Bereichs Personenidentität und Bürgerrechte
VDA:	<i>Vertrauensdiensteanbieter</i> ; ein Dienst, der elektronische Signaturen, Siegel oder Zertifikate erstellt, überprüft und validiert sowie aufbe- wahrt ¹⁸⁵
vgl:	vergleiche

¹⁸² Vgl § 2 Z 8 E-GOVG.

¹⁸³ Siehe erläuternd <https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde> (abge- rufen am 24.08.2023).

¹⁸⁴ Siehe etwa Art 24, 32 DSGVO.

¹⁸⁵ https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/anbieter/liste_der_vertrauensdiensteanbieter/Anbie- ter.de.html (abgerufen am 24.08.2023).

VO:	Verordnung
Z:	Ziffer
zB:	zum Beispiel
ZMR:	Zentrales Melderegister
Zsh:	Zusammenhang