Ausweisplattform
Datenschutz-Folgenabschätzung

Research Institute – Digital Human Rights Center

Ausweisplattform

Datenschutz-Folgenabschätzung

Bericht zur Datenschutz-Folgenabschätzung betreffend die Ausweisplattform im Auftrag des Bundesministeriums für Finanzen (BMF)

Wien, September 2023

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

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

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	12.07.2023	V 0.1	Erstellung der internen Berichts-struktur	Jan Hospes	Berichtsstruktur
2	04.08.2023	V 0.3	Aufschlag für die Ausweisplattform betreffende DSFA	Jan Hospes	in Arbeit
3	08.08.2023	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 hinsicht-lich Sachverhaltes, Entwurf Risikobe-urteilung	Jan Hospes	in Arbeit
6	22.08.2023	V 0.7	Einarbeitung Risikobeurteilung	Jan Hospes	in Arbeit
7	24.07.2023	V 0.7a	Feedback zu den Bearbeitungen sei-tens BMF und BRZ	Patrick Silli	Feedback
8	24.07.2023	V 0.7b	Einarbeitung des Feedbacks	Jan Hospes	in Arbeit
9	24.08.2023	V 0.8a	Einarbeitung diverser Ergänzungen und Anmerkungen	Christof Tschohl	Review
10	24.08.2023	V 0.8b	Einarbeitung Review	Jan Hospes	in Arbeit
11	25.08.2023	V 0.8c	Einarbeitung diverser Ergänzungen und Anmerkungen	Walter Hötzendorfer	Review
12	25.08.2023	V 1.0	Einarbeitung Review	Jan Hospes	Final

Disclaimer

Sofern im Folgenden nicht anders angegeben, wurden alle Internetlinks zuletzt am 25.08.2023 abgerufen.

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

Inhalt

1 Management Summary

Der vorliegende Bericht dokumentiert die Ergebnisse der Datenschutz-Folgenabschätzung (DSFA) betreffend die **Ausweisplattform**. Die Ausweisplattform ist die technische Grundlage für die Einführung digitaler Ausweise und Nachweise. In erster Ausbaustufe ermöglichte sie es Führerscheininhaber*innen, ihren Führerschein digital mittels der eAusweise-App sowohl gegenüber Privaten als auch im Zuge von Verkehrskontrollen gegenüber Exekutivorganen vorzuweisen. Zu dieser ersten Ausbaustufe der Ausweisplattform wurde – gemeinsam mit der Funktion digitaler Führerschein - eine Datenschutz-Folgenabschätzung durchgeführt.[1] Basierend auf diesem Dokumentationsstand wird im vorliegenden Bericht eine Datenschutz-Folgenabschätzung dokumentiert, welche spezifisch ausschließlich die Ausweisplattform als Grundlagentechnologie für Ausweisfunktionen beleuchtet. Eine eigenständige Datenschutz-Dokumentation – zunächst losgelöst von den Einzelnen Anwendungsfällen – erscheint nunmehr geboten, da die Ausweisplattform mittlerweile in Richtung prinzipieller Multi-Ausweis-Fähigkeit erweitert wird und nicht mehr bloß die technische Grundlage für den digitalen Führerschein, sondern auch für neue Funktionen (zB digitaler Altersnachweis) bildet.

Die Ausweisplattform baut auf dem ID Austria System auf, hinsichtlich dessen ebenfalls gesondert eine DSFA durchgeführt und der DSFA-Bericht veröffentlicht wurde.[2] Dieses System erweitert die bisher bekannten Nutzungsmöglichkeiten von Handy-Signatur und Bürgerkarte, sodass künftig neben dem Minimaldatensatz (MDS), bestehend aus Vor-, Nachname und Geburtsdatum, auch weitere Personenmerkmale (Attribute) verarbeitet werden können. Die Möglichkeit, physische Ausweise und Nachweise zu verwenden, bleibt wie bisher unverändert und uneingeschränkt bestehen. Der *Verantwortliche* hat entschieden, schon allein aufgrund der Bedeutung der vorliegenden Materie und der hohen Sensibilität für Datenschutz, auch für die Infrastruktur der AWP selbst jedenfalls eine DSFA durchzuführen. Diese wurde durchgeführt und ist im vorliegenden Bericht dokumentiert.

Der Gegenstand der DSFA und folglich der Bericht gliedern sich in folgende Verarbeitungstätigkeiten:

- Einrichten der eAusweise-App und laden von Aus- bzw Nachweisen;
- Widerruf des Gerätezertifikats AWP;
- Abmelden von der eAusweise-App;
- Überprüfen des Aus- bzw. Nachweises

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

[1] Digitaler Führerschein - Datenschutz-Folgenabschätzung, https://www.oesterreich.gv.at/dam/jcr:272fc1f7-1a2e-451e-8a19-98e6ba137843/DSFA-Bericht%20Digitaler%20Fuehrerschein.pdf (abgerufen am 04.08.2023).

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

Potenzial zur Überwachung und die dagegen getroffenen Maßnahmen behandelt. Weiters thematisiert werden Fragen der Freiwilligkeit der Nutzung des Systems und das Thema einer möglichen Überforderung der betroffenen Personen, die Datenverarbeitung und ihre Konsequenzen zu verstehen. In der Analyse zeigt sich, dass seitens der Verantwortlichen bereits ab Beginn der Planung des Systems zahlreiche technische und organisatorische Maßnahmen ergriffen wurden, um die Risiken zu verringern sowie besser zu beherrschen und die Einhaltung der Grundsätze des Datenschutzrechts zu gewährleisten. Die vorliegende DSFA gelangt zum 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;
- die Protokollierung auf das technisch notwendige Minimum beschränkt ist und insbesondere Vorgänge des Vorweisens und Überprüfens von Ausweisen im System der Ausweisplattform nicht protokolliert werden.

Der DSFA-Bericht gelangt daher 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 nachvollziehbar 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 Datenschutz-Folgenabschätzung (DSFA) betreffend die aktuelle technische Ausgestaltung der Ausweisplattform des BMF. 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 bei der Aktualisierung der vorliegenden Dokumentation zur Datenschutz-Folgenabschätzung (DSFA) hinsichtlich der Ausweisplattform welche 2022 gemeinsam mit der Einführung des digitalen Führerscheins dokumentiert wurde.

Die Beiziehung 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. Die vorliegende Aktualisierung der bereits vorliegenden DSFA zur Ausweisplattform und dem digitalen Führerschein ist Ausfluss dieses Verständnisses da die vorliegende Aktualisierung der DSFA gerade aufgrund technischer Aktualisierungen der Ausweisplattform erfolgt. 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 insbesondere[3] 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 Straftaten[5] (gem Art 10 DSGVO) durchgeführt wird;
- oder eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche vorgenommen wird.

Darüber hinaus haben die Aufsichtsbehörden eine Liste mit Verarbeitungsvorgängen 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 Daten[8] 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 anderem[10] 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 Bedeutung, die er dem Datenschutz beimisst, in jedem Fall eine DSFA durchzuführen. Diese wurde durchgeführt und ist im vorliegenden Bericht dokumentiert.

---

[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 Berichterstattung bzgl eines Prozesses sein können, auch wenn in diesem keine Straftat festgestellt wird, siehe hierzu: EuGH, C-136/17, ECLI:EU:C:2019:773.

[6] *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 39.

[7] Vgl *Trieb* in *Knyrim,* DatKomm Art 35 DSGVO Rz 47, 69; Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) BGBl II 2018/278; Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) BGBl II 2018/108.

[8] 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).

3 Darstellung des Sachverhalts und Spezifizierung des Prüfgegenstands

Mit der Novellierung des E-Government-Gesetzes[11] 2017 kam es zu einer Weiterentwicklung von „Bürgerkarte“ bzw „Handy-Signatur“ zum „E-ID“.[12] Unter der Bezeichnung „ID Austria“ wird dieser elektronische Identitätsnachweis nunmehr zur eindeutigen Identifikation der Bürger*innen gegenüber digitalen Anwendungen und Diensten sowohl aus dem behördlichen als auch privaten Umfeld eingeführt. Durch den E-ID soll es Bürger*innen möglich sein, sich online auszuweisen, digitale Services zu nutzen und Geschäfte rechtsverbindlich auf elektronischem Wege abzuschließen.

Dabei wurden die bisher bekannten Nutzungsmöglichkeiten von Handy-Signatur und Bürgerkarte mit Einführung der ID Austria erweitert, sodass künftig neben dem Minimaldatensatz (MDS) bestehend aus Vor-, Nachname und Geburtsdatum auch weitere Personenmerkmale (Attribute) verarbeitet werden können.[13]

Durch § 4 Abs 6 E-GovG wurde zudem die Möglichkeit eines vereinfachten Nachweises von Attributen bzw entsprechender Speicherung zum E-ID geschaffen, wodurch Attributsdaten offline gespeichert und Dritten vorgewiesen werden können sollen.

Die in den beiden vorstehenden Absätzen beschriebenen Nutzungsmöglichkeiten stellen die Kernfunktionalitäten dar, auf die sich die vorliegende DSFA bezieht und auf deren Komponenten im Folgenden noch näher eingegangen wird.

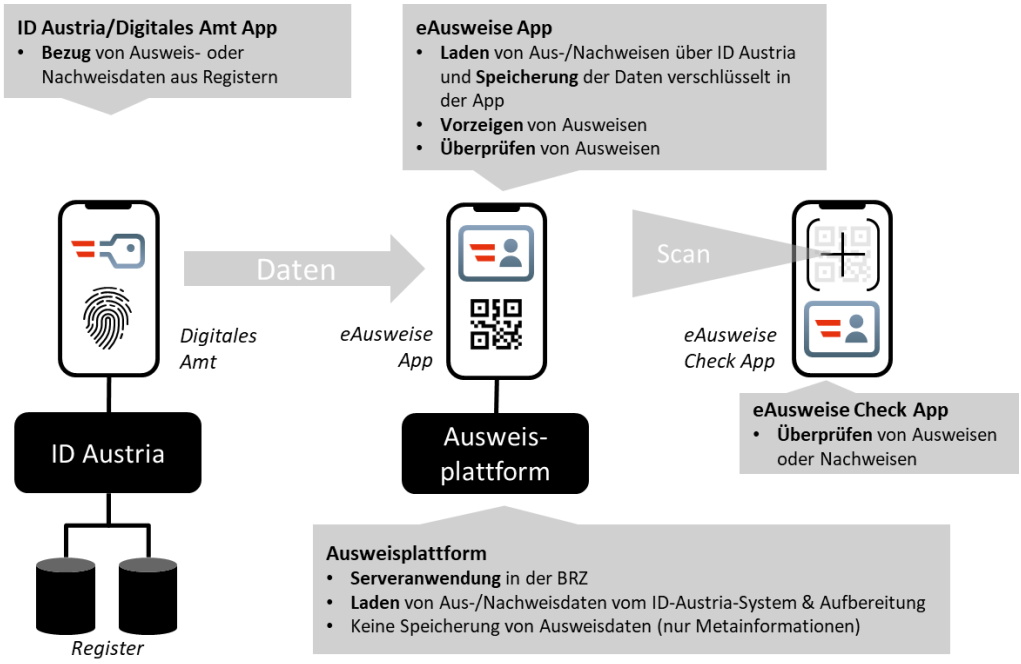

Abbildung 1: Überblick über die Systemteile

[11] E-Government-Gesetz BGBl I 2004/10 idF BGBl I 2017/121.
[12] Ein elektronischer Identitätsnachweis ist gem § 2 Z 10 E-GovG definiert als eine logische Einheit, die eine qualifizierte elektronische Signatur mit einer Personenbindung und den zugehörigen Sicherheitsdaten und -funktionen verbindet.
[13] Vgl ErläutRV 469 BlgNR 27. GP 2. Gemäß § 4 Abs 1 E-GovG dient der E-ID *„[...] dem Nachweis der eindeutigen Identität, weiterer Merkmale sowie des Bestehens einer Einzelvertretungsbefugnis eines Einschreiters und der Authentizität des elektronisch gestellten Anbringens in Verfahren, für die ein Verantwortlicher des öffentlichen Bereichs eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet hat.“*

Ausweisplattform (AWP)

Im Zuge der Realisierung des digitalen Führerscheins wurde das System der Ausweisplattform entwickelt und wurde mit dem digitalen Nachweis des Alters zur Multi-Ausweis-Fähigkeit ausgebaut. Die Ausweisplattform stellt das serverseitige Herzstück des Systems dar, wie aus Abbildung 1 hervorgeht. Sie dient als Bindeglied zwischen der ID Austria und der eAusweise-App indem sie mittels ID-Austria bezogene Daten aufbereitet und an die eAusweise-App übermittelt.

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

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 Aus- bzw Nachweisen 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 Aus- bzw Nachweisen, 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.

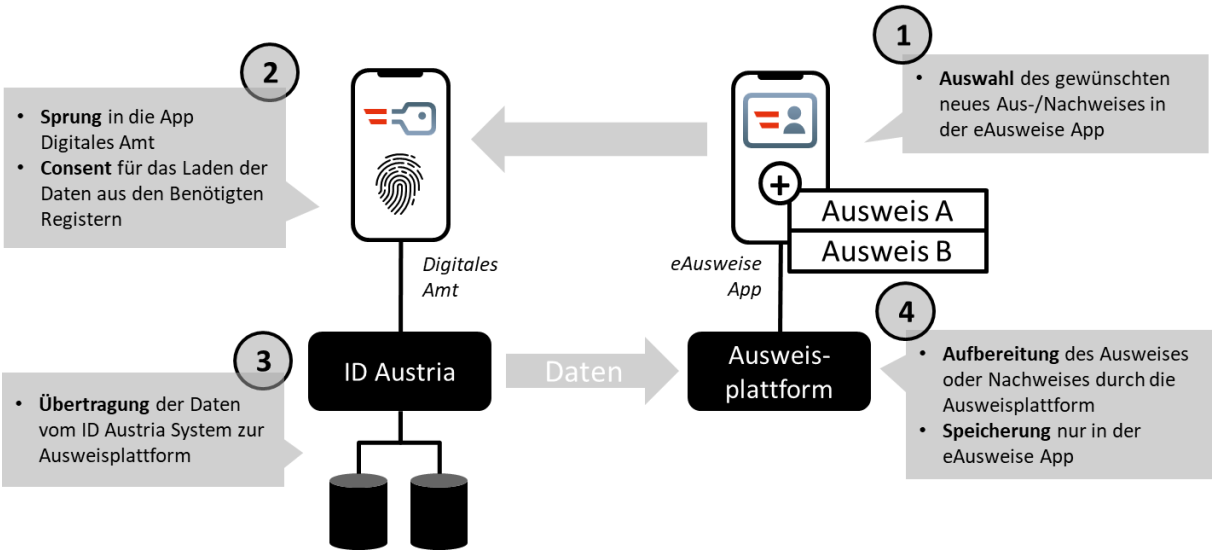

Abbildung 2: Überblick über die Funktionsweise eAusweise-App/Ausweisplattform

Durch das vorgesehene Konzept ist gewährleistet, dass die entsprechenden Ausweis- bzw Nachweisdaten aus dem entsprechenden Register nur verschlüsselt in der eAusweise-App der Nutzer*innen gespeichert werden, nicht jedoch auch in der Ausweisplattform. In der Ausweisplattform werden nur Metainformationen (wie etwa welcher Ausweis bzw Nachweis von welcher Nutzer*in geladen wurde) gespeichert. Jeder Aus- bzw. Nachweis bildet einen eigenständigen Verarbeitungszweck und wird im Zuge der Einführung spezifisch (gegebenenfalls im Rahmen einer Datenschutz-Folgenabschätzung) beleuchtet.

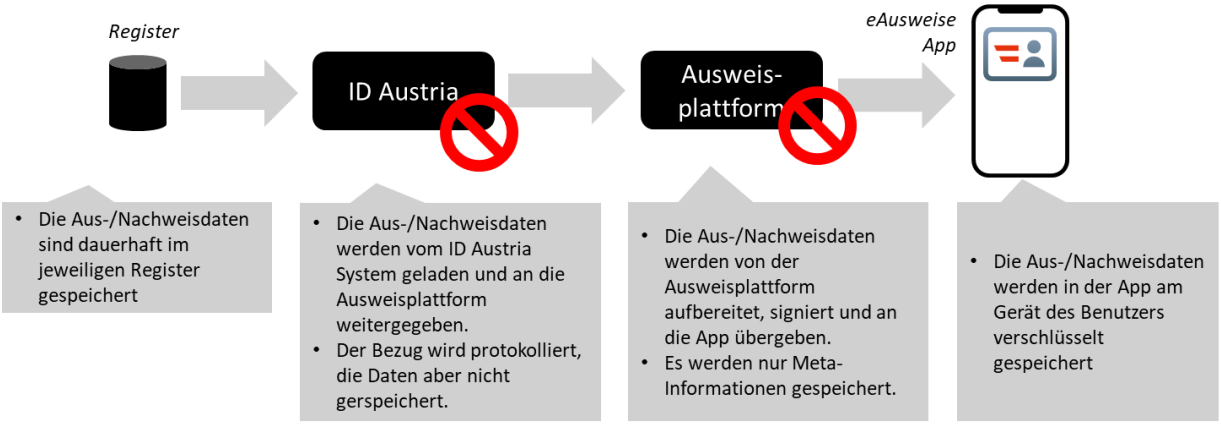

Abbildung 3: Überblick über die Speicherorte von Daten

Die eAusweise-App bietet auch die Funktionalität zum Überprüfen von digitalen Aus- und Nachweisen, die eine andere Person mit ihrer eAusweise-App vorzeigt. Die App ist (kostenlos) via Download über den „Play Store“ von Google sowie den „App Store“ von Apple erhältlich. Die eAusweise-App ist ein Angebot, das Bürger*innen optional anstelle von physischen Ausweisen verwenden können. Es besteht für niemanden eine Pflicht oder ein faktischer Zwang, die eAusweise-App anstelle eines physischen Ausweises zu verwenden. Die Verwendbarkeit von physischen Ausweisen erfährt durch die eAusweise-App keinerlei Einschränkungen.

3.1 Technische Architektur

Die folgende Darstellung zeigt die Architektur des Systems und setzt die einzelnen Komponenten in Beziehung. Diese sind nachfolgend im Einzelnen beschrieben.

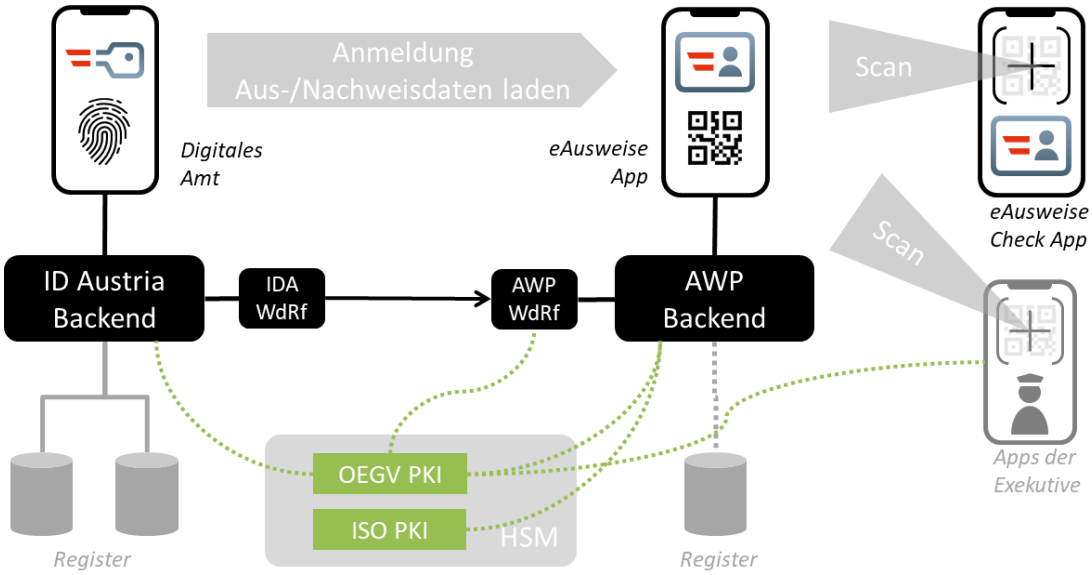

Abbildung 4: Architektur des Systems und Schnittstellen zwischen den einzelnen Komponenten

Ausweisplattform (AWP) Backend

Das Ausweisplattform-Backend-Service wird im Bundesrechenzentrum betrieben und führt alle notwendigen Operationen für den Bezug von Ausweisdaten durch.

AWP Widerrufsservice (AWP WdRf)

Das Widerrufsservice der Ausweisplattform wird vom Widerrufsservice der ID Austria über einen Widerruf der ID Austria durch eine Nutzer*in notifiziert und führt dann alle notwendigen Operationen durch.

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

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 Aus- bzw Nachweisen 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 Aus- bzw Nachweisen, die eine andere Person mit ihrer eAusweise-App vorzeigt.

ID Austria Widerrufsservice (IDA WdRf)

Das ID Austria-Widerrufsservice führt alle notwendigen Operationen bei Widerruf der ID Austria/E-ID durch, zB die Notifizierung des Ausweisplattform-Widerrufsservice.

HSM - Hardware Security Module

Die App-Zertifikate für die Apps "Digitales Amt" und "eAusweise-App" sowie die Signatur-Zertifikate für digitale Aus- bzw Nachweise (technische Bezeichnung: Document Signer Zertifikate und die PKI-Zertifikate für die Bindungszertifikate) werden in einem abgeschotteten Hardware-Sicherheits-Modul im Bundesrechenzentrum ausgestellt und verwaltet.

ID-Austria Backend

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

3.2 Prüfgegenstand

Gegenstand der vorliegenden DSFA sind daher die nachfolgend angeführten Verarbeitungstätigkeiten:

- **Einrichtung der eAusweise-App und laden von Aus- bzw. Nachweisen;**[14]
- **Widerruf des Gerätezertifikats AWP;**[15]
- **Abmelden von der eAusweise-App;**[16]
- **Überprüfen des Aus- bzw. Nachweises.**[17]

Laden, Anzeigen und Aktualisieren von Nach- bzw. Ausweisen, spezifische Prüfmethoden sowie Schnittstellen zu konkreten Registern unterscheiden sich je nach Art der zu ladenden Ausweise bzw. Nachweise und werden für eine bessere Übersichtlichkeit in jeweils eingeständigen DSFA-Berichten beleuchtet.

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 Einrichten der eAusweise-App und laden von Aus- bzw Nachweisen

Zweck dieser Verarbeitungstätigkeit ist das Laden eines Nach- oder Ausweises in die eAusweise-App der Nutzer*in, sodass sie dieser für die Verwendung zur Verfügung steht.

[14] Siehe dazu im Detail 3.3.1.
[15] Siehe dazu im Detail 3.3.2.
[16] Siehe dazu im Detail 3.3.3.
[17] Siehe dazu im Detail 3.3.4.

Zur initialen Einrichtung der eAusweise-App muss die Nutzer*in zunächst den Nutzungsbedingungen zustimmen und bestätigen, dass er*sie die Datenschutzinformation zur Kenntnis genommen hat. Um sich in weiterer Folge neuerlich an der eAusweise-App anmelden zu können, muss sich die Nutzer*in biometrisch authentisieren, um diese Login-Methode für die App einzurichten. Erfolgt dies nicht, kann die eAusweise-App nicht verwendet werden. Mit anderen Worten, die Verwendung der biometrischen Authentisierung[18] ist Voraussetzung für die Nutzung der eAusweise-App.

Voraussetzung für das Laden von Aus- bzw. Nachweisen ist, dass auf demselben Endgerät auch die Digitales-Amt-App installiert ist. Ist dies nicht der Fall, wird die Nutzer*in bei der Anmeldung zur Installation der Digitales-Amt-App aufgefordert. Ist diese installiert, wird die Nutzer*in in die App "Digitales Amt" weitergeleitet.

Somit handelt es sich hierbei um die Anmeldevariante "Anmeldung aus Third-Party-App mit Anmeldeziel Third-Party-App" der ID Austria, die hier im Detail wie folgt abläuft:

Die Nutzer*in befindet sich dabei zunächst in der eAusweise-App, die sich **am selben** Gerät wie die Digitales-Amt-App befindet. Die eAusweise-App agiert im Rahmen der ID Austria als Service Provider (SP). Die eAusweise-App bzw. das AWP-Backend erstellt einen Authentifizierungs-Request (also eine Anfrage), der an die Digitales-Amt-App und von dort weiter an den Identity Provider der ID Austria (IDP) übermittelt wird.

Nach erfolgter Authentifizierung stellt der IDP einen Registrierungstoken aus und übermittelt diesen an die eAusweise-App und die Nutzer*in wird in die eAusweise-App geleitet. Die Ausweisplattform nimmt den Registrierungstoken entgegen, validiert diesen und lädt daraufhin die für den Aus- bzw.-Nachweis erforderliche Attribute vom ID-Austria System. Daraufhin wird der Registrierungstoken in der Ausweisplattform gelöscht. Die Daten werden entsprechend aufbereitet und an die eAusweise-App übermittelt. Nur dort werden die Ausweisdaten dann verschlüsselt gespeichert.

Der für die Authentifizierung verwendete Standard ist OpenID Connect (OIDC).

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
- bPK[19]
- IP-Adresse des Mobilgeräts
- Status der ID Austria (Voll- oder Basisfunktion)
- Registrierungstoken (ID-Token)

[18] Siehe dazu die Behandlung der mit biometrischer Authentisierung verbundenen Risiken unter 5.2.2 sowie 5.2.6.

[19] 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).

Folgende Daten werden hierbei erhoben und am Endgerät gespeichert:

- Funktionsspezifische Attribute (zB Altersstufe, Lichtbild…)[20]
- Signaturzertifikat

3.3.2 Widerruf des Gerätezertifikats AWP

Zweck dieser Verarbeitungstätigkeit ist es, für den Fall, dass die ID Austria einer Person abläuft oder ungültig wird, auch die Anmeldung in der eAusweise-App dieser Person sowie die aktuell in die App geladenen Aus- bzw. Nachweise für ungültig zu erklären, da die eAusweise-App nur mit gültiger ID Austria verwendet werden kann.

Der Widerruf des Gerätezertifikats für die Ausweisplattform erfolgt durch den Widerruf der jeweiligen ID Austria der Nutzer*in, welcher wiederum auf verschiedene Arten erfolgen kann.[21] Hierbei wird im Backend das jeweilige bPK vom ID Austria System an die Ausweisplattform übermittelt. Daraufhin wird das Gerätezertifikat der entsprechenden Nutzer*in auf eine Widerrufsliste (Certificate Revocation List, CRL) gesetzt. Diese ist implementiert als Standard-X.509v2-CRL[22] und enthält im Wesentlichen die Seriennummern der widerrufenen Zertifikate. Der Personenbezug dieser Seriennummer kann nur in der AWP sowie durch die Prüf-app im Zuge der Überprüfung des Ausweises der jeweiligen betroffenen Person hergestellt werden. Die Widerrufsliste wird beim Start der jeweiligen Prüf-App stets neu vom Server geladen und bei einem Prüfvorgang mit dem Gerätezertifikat der jeweiligen Nutzer*in abgeglichen. Befindet sich das Gerätezertifikat der überprüften Person auf der Widerrufsliste, schlägt die Ausweisprüfung fehl. Kann die aktuelle Widerrufsliste beim Start der Prüf-App nicht geladen werden, insbesondere weil keine Internetverbindung besteht, und ist die zuletzt geladene Widerrufsliste bereits älter als 48 Stunden, so kann die Ausweisprüfung zwar durchgeführt werden, es wird allerdings ein Hinweis angezeigt, dass die Widerrufsliste veraltet ist.

Folgende Daten werden hierbei verarbeitet:

- bPK-ZP
- Seriennummer des Gerätezertifikats

3.3.3 Abmelden von der eAusweise-App

Zweck dieser Verarbeitungstätigkeit ist das Löschen von Daten der Nutzer*in auf dem entsprechenden Endgerät bzw serverseitig durch die Nutzer*in selbst. Da der geladene Aus- bzw Nachweis lediglich in der eAusweise-App gespeichert ist, wird ein “Widerruf” des Aus- bzw Nachweises, wenn von der betroffenen Person gewünscht, schlicht durch das Löschen dieser Daten durch die betroffene Person in der eAusweise-App bewirkt. Hierzu wählt die Nutzer*in “Dieses Gerät abmelden” in der eAusweise-App aus. Daraufhin werden jedenfalls alle am Gerät gespeicherten Daten gelöscht. Handelt es sich beim entsprechenden Gerät um das Einzige der Nutzer*in, das im Zusammenhang mit der eAusweise-

[20] Je nachdem, welcher digitale Ausweis oder Nachweis geladen wird, kommt es zu unterschiedlichen Verarbeitungstätigkeiten. Details werden angezeigt, bevor Ladevorgang gestartet wird. Hinsichtlich dieser Datenverarbeitungen wird spezifisch informiert und ggf. eine Datenschutz-Folgenabschätzung durchgeführt.
[21] Insbesondere muss dieser nicht zwingend unmittelbar durch Nutzer*innen ausgelöst werden, sondern erfolgt etwa auch, wenn ein Rooting des Endgeräts erkannt wird.
[22] Siehe dazu https://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/X509CRL.html (abgerufen am 24.08.2023).

App verwendet wird, werden zudem auch alle in der Datenbank serverseitig gespeicherten Daten gelöscht. Ist dies nicht der Fall, verwendet die Nutzer*in also noch auf einem Gerät die eAusweise-App, werden serverseitig lediglich die Daten in Bezug auf jenes Gerät aus der Datenbank gelöscht.[23]

3.3.4 Überprüfen des Aus- bzw. Nachweises

Die eAusweise-App umfasst zudem auch die Funktion, um einen Ausweis offline zu überprüfen. Hierzu bedarf es keiner Anmeldung der überprüfenden Person mittels ID Austria an der eAusweise-App. Bei der Überprüfung selbst werden keine personenbezogenen Daten der überprüfenden Person verarbeitet, sie bleibt während des Prüfprozesses anonym.[24]

Daneben können Prüfungen auch mittels eAusweis Check-App erfolgen. Diese ist im Funktionsumfang auf die Überprüfung von Attributen einer anderen Person eingeschränkt und ermöglicht – im Gegensatz zur eAusweise-App - keine Registrierung an der ID-Austria und damit kein Laden von Nach- bzw. Ausweisen. Im Zuge der Überprüfung werden keine personenbezogenen Daten der Nutzer*innen verarbeitet. Die eAusweis Check-App ermöglicht Nutzer*innen ihre informationelle Selbstbestimmung maximal zu wahren.

Verarbeitungen personenbezogener Daten der *zu überprüfenden* Person werden im Rahmen der zu den einzelnen Funktionen durchgeführten Datenschutz-Folgenabschätzungen abgehandelt.

[23] Diesfalls würden etwa Informationen darüber, welche Aus- bzw Nachweise die Nutzer*in bezogen hat, gespeichert bleiben.
[24] Die überprüfende Person kann daher auch mittels eAusweise-App anonym prüfen.

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.[25]

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);
- Verhältnis zu Auftragsverarbeitern (Art 28);
- Garantien in Bezug auf die internationale Übermittlung von Daten.[26]

[25] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 112; siehe auch *Bock* et al, Datenschutz-Folgenabschätzung für die Corona-App (2020) 60 ff.
[26] Siehe *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01 (2017) 28 f.

4.1 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.[27] 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.[28] 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.[29]

Vor allem auch in Bezug auf Datenverarbeitungen durch Endgeräte wie Smartphones und Tablets, ist zu berücksichtigen, dass Standortinformationen, eindeutige Geräte- und Kundenkennungen (wie zB IMEI[30], IMSI[31], UDID[32], MSISDN[33]), die Identität des Telefons[34], Kreditkarten- und Zahlungsdaten oder auch der Browserverlauf als personenbezogene Daten zu werten sind.[35] Weitere gängige Angaben mit identifizierendem Bezug zu einer natürlichen Person sind zB Handynummer[36], E-Mail-Adresse, Sozialversicherungsnummer[37], KFZ-Kennzeichen[38], IP-Adresse[39] und auch medizinische Diagnosen.[40]

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.[41] Die Information kann sich zusammensetzen aus sachbezogenen Aussagen zu Verhältnissen oder überprüfbaren Eigenschaften sowie Einschätzungen und Urteilen über die betroffene Person. Der Personenbezug von Daten kann wiederum durch jene Information hergestellt werden, welche ein Inhaltselement, Zweckelement oder Ergebniselement beinhaltet. Der dritte wesentliche Faktor bei der Qualifikation von personenbezogenen Daten gem Art 4 Z 1 DSGVO richtet sich auf die betroffene Person,

---

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

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.[42] 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.[43] 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.*"

Die Literatur[44] und unionsrechtliche Judikatur[45] setzen am sogenannten „*relativen Personenbezug"* bzw der "*relativen Theorie*"[46] an, wonach für die Bestimmung der Identifizierbarkeit die Kenntnisse und Mittel der datenverarbeitenden Stelle und nicht irgendeines *Dritten* ausschlaggebend sind. Sofern

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

der *Verantwortliche* Einzelangaben einer Person durch relevantes Zusatzwissen[47] [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.[48] 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.*"[49]

4.1.2 Personenbezogene Daten im System

Auf Basis der eben dargestellten rechtlichen Grundlagen ist im gegenständlichen Fall daher grundsätzlich (sofern nicht ausdrücklich Gegenteiliges beschrieben wird) 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.[50] 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,[51] 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.

[47] 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).
[48] Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.
[49] EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779, Rz 65.
[50] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.
[51] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] 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.[52] Für die Verarbeitung von personenbezogenen Daten gem Art 4 Z 1 DSGVO enthält Art 6 Abs 1 DSGVO eine taxative Liste von sechs Erlaubnistatbeständen woraus für den Betrieb der Ausweisplattform insbesondere die Verarbeitung aufgrund nationalgesetzlicher Bestimmungen iSd Art 6 Abs 1 lit e DSGVO bzw. im Falle besonderer Kategorien personenbezogener Daten[53] (kurz: sensibler Daten) Art 9 Abs 2 lit g DSGVO. Im Folgenden ist dokumentiert, wie die Zulässigkeit der einzelnen oben angeführten Verarbeitungstätigkeiten begründet wird.

4.2.2 Einrichten der eAusweise-App und laden von Aus- bzw Nachweisen

Die Rechtsgrundlage der Übermittlung des Minimaldatensatzes ist Art 6 Abs 1 lit e DSGVO. Diese Bestimmung legt fest, dass die Verarbeitung rechtmäßig ist, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem *Verantwortlichen* übertragen wurde.

Eine solche Rechtsgrundlage muss dabei durch Unionsrecht oder das Recht des betreffenden Mitgliedstaats festgelegt werden, dem der *Verantwortliche* unterliegt. Art 6 Abs 1 lit e steht in einem engen Zusammenhang mit Art 6 Abs 2 und 3, wonach der Zweck zur Erfüllung der gesetzlich übertragenen Aufgabe notwendig sein muss. Letztere muss in der Rechtsgrundlage hinreichend bestimmt beschrieben werden. Da Art 6 Abs 1 lit e ein sehr weit gefächertes Anwendungsspektrum besitzt, ist laut Artikel-29-Datenschutzgruppe *„eine strenge Auslegung und eine klare Benennung des gegebenen öffentlichen Interesses und der öffentlichen Gewalt, die die Verarbeitung rechtfertigen, auf Einzelfallbasis geboten."*[54]

Die nationalen Rechtsgrundlagen sind die §§ 4 iVm 4b iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG. Diese Datenverarbeitung ist ein konkreter Anwendungsfall der Verarbeitungstätigkeit "Verwendung der ID Austria" des ID Austria Systems. Für die Übermittlung zusätzlicher Attribute bzw Merkmale iSd § 4 Abs 2 E-GovG wird entsprechend der Einwilligung der betroffenen Person eingeholt. Die Übermittlung des Minimaldatensatzes inklusive bPK ist durch §§ 4 Abs 5 iVm 4b Abs 1 E-GovG gedeckt.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[55] aus:

„Es soll eine Definition für den Verwendungsvorgang des E-ID eingeführt werden. Diese soll klarstellen, dass bei der Verwendung des E-ID die Erstellung einer Personenbindung entweder so wie schon derzeit mittels qualifizierter elektronischer Signatur des E-ID-Inhabers oder alternativ mittels eines sicherheits-

[52] Vgl *Feiler/Forgó*, EU-DSGVO Art 6 Anm 1.
[53] Gem Art 9 Abs 1, Art 4 Z 13 - 15 DSGVO.
[54] Vgl *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 45 ff (Stand 7. 5. 2020, rdb.at).
[55] ErläutRV 469 BlgNR 27. GP 2.

technisch gleichwertigen Vorgangs ausgelöst werden kann. Ein derartiger sicherheitstechnisch gleichwertiger Vorgang ist notwendig, um künftig die Smartphone-basierte Auslösung der E-ID Funktion am selben Gerät wie die Anwendung, zu der die Authentifizierung erfolgen soll, in einer sicheren Art und Weise durchführen zu können.

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

Die biometrischen Daten werden ausschließlich gemäß den geltenden technischen Standards der Hersteller auf dem Endgerät des Benutzers verarbeitet. Eine Verarbeitung dieser Daten außerhalb des Endgeräts erfolgt zu keinem Zeitpunkt.

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

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

Zudem führen die Materialien[56] aus:

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

[56] ErläutRV 469 BlgNR 27. GP 7.

4.2.3 Widerruf des Gerätezertifikats AWP

Die Verarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO. Da der Widerruf des Gerätezertifikats der AWP technisch am Widerruf der ID Austria anknüpft, bildet § 4a Abs 5 E-GovG auch hier die Rechtsgrundlage.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien aus:[57]

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

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

4.2.4 Abmelden von der eAusweise-App

Hierbei handelt es sich um einen durch die betroffene Person ausgelösten Löschvorgang ihrer personenbezogenen Daten. Sohin bedarf es keiner gesonderten Rechtsgrundlage.

4.2.5 Überprüfen des Aus- bzw. Nachweises

Die eAusweise-App setzt technisch nicht voraus, dass personenbezogene Daten der überprüfenden Person verarbeitet werden. Eine Anmeldung ist nur für das Laden von Ausweisen notwendig.

Bei Verwendung der eAusweis Check-App werden keine personenbezogenen Daten der überprüfenden Person verarbeitet, weshalb keine datenschutzrechtliche Rechtsgrundlage erforderlich ist.

Auf Rechtsgrundlagen hinsichtlich der Verarbeitung personenbezogener Daten der überprüften Person wird im Rahmen der jeweiligen Ausweisfunktion abgehandelt.

[57] ErläutRV 469 BlgNR 27. GP 4.

4.3 Rollenverteilung nach Maßgabe der DSGVO

4.3.1 Allgemeine Systematik der Rollenverteilung

Grundlegend festzuhalten ist, dass die Eruierung der jeweiligen datenschutzrechtlichen Rolle 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;[58] 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*"[59] 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.[60]

Sofern jedoch zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, führt dies zur sogenannten "*pluralistische*[n] *Kontrolle*"[61] 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*"[62] 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,[63] 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.[64]

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:

---

[58] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 89.
[59] *Raschauer* in *Sydow*, Europäische Datenschutzgrundverordnung[2] Art 4 Rz 123.
[60] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 83 f.
[61] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 10, 22, 38f; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 80.
[62] EuGH C-210/16 VbR 2018/109; *Gabauer/Knyrim*, Checkliste Prüfschema zur datenschutzrechtlichen Rollenverteilung, Dako 2019/8, 14 (15).
[63] *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[64] Vgl *Feiler/Forgó,* EU-DSGVO Art 26 Anm 3.

- *Namen und Kontaktdaten aller Verantwortlichen*[65]
- *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;*[66]
- *gegebenenfalls Benennung eines Verantwortlichen als zentrale Anlaufstelle nach Art 26 Abs 1 S 3*.[67]

An der jeweiligen Verarbeitung kann auch ein ***Auftragsverarbeiter*** mitwirken, der dem *Verantwortlichen* stets als *„verlängerter Arm"*[68] dient. Dies, da der *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, als rechtlich eigenständige und externe Organisation,[69] Datenverarbeitungstätigkeiten lediglich „im Auftrag" des *Verantwortlichen* durchzuführen hat. Daher kommt dem *Auftragsverarbeiter* grds keine Entscheidungsbefugnis hinsichtlich der Verarbeitungszwecke und (wesentlichen) -mittel zu.[70] 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.[71] Jedoch liegt die Entscheidungskompetenz über die „wesentlichen Mittel" der Verarbeitung stets beim *Verantwortlichen*.[72]

Die dem *Verantwortlichen* oder *Auftragsverarbeiter* unterstellten Personen gelten grds als ihnen *„zurechenbare Personen"*[73], da sie idR nur als *„Ausführungsorgan"* für den *Verantwortlichen* oder *Auftragsverarbeiter* tätig sind.[74] Dies gilt jedoch nur solange sie sich an die Vorgaben bzw vorab festgelegten Zwecke und Mittel der Verarbeitung halten.

---

[65] *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.
[66] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[67] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41.
[68] *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter – was ändert sich mit der DSGVO? ZTR 2017, 59 (59).
[69] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 30.
[70] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 94.
[71] *Hartung* in *Kühling/Buchner*, DS-GVO/BDSG[2] Art 4 Nr 7 Rz 13; *Feiler/Forgó*, EU-DSGVO Art 4 Anm 12; *Artikel-29-Datenschutzgruppe,* Stellungnahme 1/2010, 17.
[72] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 17 f.
[73] 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.
[74] *Bergauer* in *Bergauer/Jahnel/Mader/Staudegger* (Hrsg), jusIT Spezial: DS-GVO (2018), 31 (38).

Zum ***Empfänger*** gem Art 4 Z 9 DSGVO zählt potenziell fast jeder datenverarbeitende Akteur,[75] der zumindest ein „gewisses Maß an Eigenständigkeit“[76] aufzuweisen hat und dem personenbezogene Daten innerhalb einer Verarbeitungstätigkeit lediglich offengelegt werden.

Ferner gibt es auch die Rolle des „außenstehenden“[77] ***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.[78] Es kann daher jeder lebende[79] Mensch die Rolle der betroffenen Person einnehmen, unabhängig von einer spezifischen Voraussetzung iS eines bestimmten Alters oder Geisteszustands.[80]

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.[81] 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.[82]

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.[83]

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.[84] Daher richtet sich der grundrechtliche Schutz gem § 1 DSG auch auf juristische Personen, wodurch nach systematischer Interpretation der Begriff „betroffene Personen“

---

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

[76] 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.

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

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

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

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

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

[82] 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.*“

[83] 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.

[84] *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.

in den einfachgesetzlichen Bestimmungen des DSG auch juristische Personen erfasst.[85] 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.[86]

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) Verantwortlichen

Basierend auf der bisherigen und maßgeblichen Rechtsprechung[87] 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.[88]
- 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.[89]
- Gemeinsame Verantwortlichkeit setzt nicht voraus, dass sämtliche Verantwortliche für dieselbe Verarbeitungstätigkeit einen (gemeinsamen) Zugang zu den betreffenden personenbezogenen Daten haben müssen.[90]
- 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.[91] Daher kann die Verantwortlichkeit bestimmter Verantwortlicher in verschiedenen Phasen und in unterschiedlichem Ausmaß ausgeprägt sein, wodurch der Grad der Verantwortlichkeit variieren kann.[92] Dabei kann man von einer qualitativ differenzierten Verantwortlich-

[85] *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.
[86] *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).
[87] 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.
[88] EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317, Rz 34.
[89] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 36 ff, 39.
[90] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 38.
[91] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.
[92] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.

keit 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.[93]
- 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.[94]
- Für die Entscheidung über Zwecke und Mittel der Verarbeitung bedarf es keiner schriftlichen Anleitung oder Anweisung zur gemeinsamen Datenverarbeitung.[95]
- Eine gemeinsame Entscheidung über das Mittel der Verarbeitung (wie Social Plug-In[96]) 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.[97]
- 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.[98]
- 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.[99]

4.3.3 Rollenverteilung der Ausweisplattform

Für die Rollenverteilung in der Ausweisplattform, vor allem im Hinblick auf die Rolle des oder der *Verantwortlichen*, kommt zunächst der sogenannten "*rechtlichen Verantwortlichkeit*"[100] 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

[93] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 68, 70 ff.
[94] Vgl EuGH C-25/17 VbR 2018/110 (202).
[95] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 67.
[96] Social Plug-Ins können als Mittel der Verarbeitung angesehen werden, da durch deren Einbindung in Websites die Möglichkeit der Verarbeitung (Erhebung oder/und Übermittelung) von personenbezogenen Daten (auch durch Dritte) begründet wird -EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77.
[97] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77, 79.
[98] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 80 ff, 84.
[99] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 74, 85.
[100] *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110); *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG² Art 4 Nr 7 Rz 15.

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,[101] 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 ist vor allem § 2 Abs 1 Z 2 Bundesminsteriengesetz 1986 idF BGBl I 98/2022 (BMG) iVm Abschnitt F Z 15 des Teiles 2 der Anlage 2 zum BMG einschlägig. Dieser betraut das Bundesministerium für Finanzen mit der Besorgung der Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung für das Service und die Interaktion mit Bürgern und Unternehmen, insbesondere einschließlich ua der Angelegenheiten des E-Governments.

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“[102], zumal die vollumfängliche Verantwortung über eine Datenverarbeitung nur jener Akteur trägt, der über die Zwecke und Mittel der Verarbeitung entscheidet.[103] Diesbezüglich ist hervorzuheben, dass das BMF im Rahmen des gesetzlichen Auftrages federführend an der Parametrierung der Funktion beteiligt und nimmt damit auch wesentlichen faktischen Einfluss auf die Systemausgestaltung. Das BMF beauftragt den Betrieb der Schnittstelle zwischen Bürger und ID-Austria, weshalb es insgesamt als verantwortliche Stelle zu qualifizieren ist.

4.3.4 Einrichten der eAusweise-App und laden von Aus- bzw Nachweisen

Die Nutzer*in führt mithilfe der ID Austria einen Anmeldevorgang durch. Das BMF agiert hier als Service Owner iSd ID Austria. Das BMF ist bezüglich des Datenverkehrs zur Nutzer*in als *Verantwortlicher* iSd Art 4 Z 7 DSGVO zu qualifizieren, da es im Rahmen des gesetzlichen Auftrages (siehe 4.3.3) den Betrieb der Anmeldeschnittstelle faktisch beauftragt.

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BMF des BRZ als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, denn das BRZ betreibt die Anmeldeschnittstelle (eAusweise-App[104]), welche notwendige Funktionalitäten zur Authentifizierung von Nutzer*innen im Zuge von Anmeldeprozessen an Services und Applikationen implementiert, die über eine Anbindung zum ID Austria System verfügen. Diese Verarbeitung erfolgt im Rahmen eines Vertragswerks, abgeschlossen zwischen der BRZ GmbH und der Republik Österreich, dessen Bestandteil auch ein Auftragsverarbeitungsvertrag nach Art 28 DSGVO ist.

Verantwortlicher:

[101] Vgl *Raschauer* in *Sydow,* Europäische Datenschutzgrundverordnung² Art 4 Rz 141; *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG² Art 4 Nr 7 Rz 14.
[102] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83.
[103] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83; *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (101).
[104] Die eAusweise-App agiert als Service Provider im Rahmen der ID Austria. Siehe Abschnitt 3.3.1.

- BMF: Betrieb Ausweisplattform, Verwendung des E-ID zur Anmeldung

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform, Verwendung des E-ID zur Anmeldung

4.3.5 Widerruf des Gerätezertifikats AWP

Das BMF ist als *Verantwortlicher* gem Art 4 Z 7 DSGVO zu qualifizieren, da es den Betrieb der Schnittstelle für Widerrufe zwischen ID Austria und Ausweisplattform beauftragt.

Verantwortlicher:

- BMF: Betrieb Ausweisplattform

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.6 Abmelden von der eAusweise-App

Es liegt dieselbe Rollenverteilung vor wie bei der Verarbeitungstätigkeit „Einrichten der eAusweise-App und laden von Aus- bzw Nachweisen“ (4.3.4).

Verantwortlicher:

- BMF: Betrieb Ausweisplattform

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.7 Überprüfen des Aus- bzw. Nachweises

Es liegt keine Verarbeitung personenbezogener Daten der mittels eAusweis Check-App überprüfenden Person vor und daher ist diesbezüglich keine datenschutzrechtliche Rolle zu qualifizieren. Die Verarbeitung personenbezogener Daten der *zu überprüfenden* Person wird im Rahmen der jeweiligen Ausweisfunktion abgehandelt.

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.[105] 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.[106]

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 digitale Aus—bzw Nachweise verwendet oder ausschließlich physische Aus- bzw Nachweise.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Ausweis oder Nachweis vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten, die überdies direkt zwischen den Endgeräten ohne Einbeziehung eines Servers erfolgt.[107]
- Die Ausweisplattform wird auch künftig konsequent um weitere Funktion erweitert werden, welche es der geprüften Person ermöglichen, situativ den zweckentsprechenden Nach- bzw. Ausweis zu erbringen ohne zweckfremde Daten offenzulegen. So kann derzeit etwa zum Nachweis des Erreichens einer Altersstufe nur diese übermittelt werden (digitaler Altersnachweis).
- Die überprüfende Person muss sich nicht an der eAusweise-App anmelden oder kann überhaupt die eAusweis Check-App verwenden, sodass es zu keiner Verarbeitung ihrer personenbezogenen Daten im Zusammenhang mit der Prüfung kommt.

[105] Siehe zudem die primärrechtliche Grundlage in Art 8 Abs 2 EU-Grundrechte-Charta (GRC).
[106] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DSGVO (2018) 37.
[107] Dies etwa nicht für den Fall der Verkehrskontrolle. Zu beachten sind allerdings die bereits bisher bestehenden Befugnisse der Sicherheitsbehörden zum direkten Zugriff auf die Daten des Führerscheinregisters, die durch das Projekt digitaler Führerschein unberührt bleiben.

Somit kann die betroffene Person selbst entscheiden, zu welchen Zwecken ihre personenbezogenen Daten im Zusammenhang mit digitalen Aus- bzw Nachweisen verwendet werden und ob dies überhaupt der Fall sein soll und kann die maximale Selbstbestimmung und Kontrolle über diese Vorgänge ausüben.

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

Einrichtung der eAusweise-App und laden von Nach- bzw. Ausweisen

Wie unter 3.3.1 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit die Einrichtung der eAusweise-App auf dem Endgerät der Nutzer*in, sodass sie dieser für die Verwendung zur Verfügung steht.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Verschlüsselte Speicherung sowohl der Daten in der Ausweisplattform als auch der Daten auf dem Endgerät
- Grundsätzlich rein automatisierte Verarbeitung, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt
- Verschlüsselung der in der eAusweise-App gespeicherten Daten
- Vor dem Laden eines Ausweises 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.
- 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 Vorweisens und Überprüfen von Ausweisen im System der Ausweisplattform nicht protokolliert.
- Grundsätzlich rein automatisierte Verarbeitung, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt
- Reine Offline-Speicherung des digitalen Ausweises bzw Nachweises, womit auch einer potenziell zweckwidrigen, serverseitigen Verarbeitung vorgebeugt wird
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen

Widerruf des Gerätezertifikats AWP

Wie unter 3.3.2 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit, für den Fall, dass die ID Austria einer Person abläuft oder ungültig wird, auch die Anmeldung in der eAusweise-App dieser Person sowie die aktuell in die App geladenen Ausweise bzw Nachweise für ungültig zu erklären, da die eAusweise-App nur mit gültiger ID Austria verwendet werden kann.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Der Personenbezug der Einträge in der Widerrufsliste kann nur in der AWP sowie durch die überprüfende App im Zuge der Überprüfung des Ausweises der jeweiligen betroffenen Person

hergestellt werden und somit nur dann, wenn dies für den Zweck, dem die Widerrufsliste dient, erforderlich ist.
- Grundsätzlich rein automatisierte Verarbeitung (nach dem sog. „hit/no-hit Verfahren“), was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt

Abmelden von der eAusweise-App

Zweck dieser Verarbeitungstätigkeit ist, wie unter 3.3.3. erwähnt, das Löschen von Daten der Nutzer*in auf dem entsprechenden Endgerät bzw auf dem Server durch die betroffene Person selbst.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Nutzer*innen haben es selbst in der Hand, wann sie diesen Vorgang auslösen und zu welchem dahinterliegenden Zweck dies erfolgt.
- Dabei werden neben den in der App gespeicherten Daten zumindest die in der entsprechenden Datenbank serverseitig gespeicherten Daten in Bezug auf jedes abzumeldende Gerät gelöscht. Dies erfolgt, wenn es sich nicht um das einzige Gerät handelt, das die Nutzer*in im Zusammenhang mit der Ausweisplattform verwendet.
- Wenn das einzige bzw letzte Gerät abgemeldet wird, werden alle in der entsprechenden Datenbank serverseitig gespeicherten Daten gelöscht. Damit wird auch einer potenziell zweckwidrigen weiteren Verarbeitung dieser Daten entgegengewirkt.

Überprüfen des digitalen Aus- bzw Nachweises

Wie unter 3.3.4 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit die Verwendung der jeweiligen Funktion der eAusweise-App oder eAusweis Check-App, einen Ausweis oder Nachweis offline zu überprüfen, um so die Gültigkeit des digitalen Aus- bzw. Nachweises einer anderen Person zu prüfen.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Die Funktion, welche es ermöglicht, Ausweisdaten in der eAusweise-App ohne vorherige Anmeldung durchzuführen, ist leicht auffindbar.
- Die Bereitstellung der eAusweis Check-App stellt aber selbst eine Maßnahme dar, um die maximale informationelle Selbstbestimmung betroffener Personen zu verbessern, zumal diese demnach selbst entscheiden können, ob sie zur Prüfung von Ausweisen anderer Personen die (für diesen Zweck ebenfalls nur anonym arbeitende) eAusweise-App oder die von vornherein ausschließlich anonyme eAusweis Check-App verwenden.

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.[108] Zudem haben Verantwortliche gem Art 25 DSGVO die Pflicht, die Datenminimierung durch Technikgestaltung und datenschutzfreundliche Voreinstellungen wirksam umzusetzen.

[108] Siehe auch ErwGr 39 DSGVO.

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:

- Bereits die Architektur des Systems der Ausweisplattform folgt dem datenschutzrechtlichen Prinzip „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ und damit auch dem Grundsatz der Datenminimierung; insbesondere werden die durch die betroffene Person auf eigene Initiative geladenen Ausweis- bzw Nachweisdaten ausschließlich auf dem Endgerät der betroffenen Person gespeichert.
- Das Vorweisen und Überprüfen des Aus- bzw. Nachweises erfolgt grundsätzlich offline, dh ausschließlich auf den beiden an der Prüfung beteiligten Endgeräten, und somit ohne Auslösung einer Datenverarbeitung außerhalb der beiden verwendeten Endgeräte; zur Erforderlichkeit der ausnahmsweise davon abweichenden Implementierung der Prüfung durch Exekutivorgane wird gegebenenfalls im Zusammenhang mit der spezifischen Funktion ausgeführt.
- Die Protokollierung ist hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt; siehe dazu Abschnitt 4.6.7 unten.
- 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.

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 (s dazu 3.3.3).

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 Authentifizierung am IDP 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 beziehen, 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 der Einrichtung zusätzlich zu den zu akzeptierenden Nutzungsbedingungen die Datenschutzerklärung präsentiert. Diese kann auch danach jederzeit auf der Startseite der App 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 Link[109] 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 BMF[110] 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.[111]

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 BMF[112] 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.

---

[109] Zum Zeitpunkt der Erstellung des Berichts im angemeldeten Bereich unter https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 24.08.2023).
[110] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 24.08.2023).
[111] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 24.08.2023).
[112] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 24.08.2023).

Diese Voraussetzungen sehen ein Löschungsrecht 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 Datenschutzinformation als auch auf der entsprechenden Webseite des BMF[113] die erforderlichen Kontaktmöglichkeiten angegeben.

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 Authentifizierung am IDP vergebene Registrierungstoken werden zudem nach deren einmaliger Nutzung aus der entsprechenden Datenbank gelöscht.

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 Datenschutzerklärung[114] als auch auf der entsprechenden Website des BMF[115] 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.[116]

[113] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 24.08.2023).
[114] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html (abgerufen am 24.08.2023).
[115] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 24.08.2023).
[116] 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 Datenschutzrechtliche Anforderungen an die Protokollierung

Bevor im Rahmen dieses DSFA-Berichts auf die konkrete Ausgestaltung der Protokollierung mit Fokus auf die Risikoanalyse eingegangen wird, sollen im Folgenden die datenschutzrechtlichen Rahmenbedingungen[117] überblicksartig dargestellt werden.

Vorauszuschicken ist bereits an dieser Stelle, dass der Begriff der Protokollierung in der DSGVO nicht ausdrücklich genannt wird. Die Vornahme einer Protokollierung von Verarbeitungsvorgängen kann sich jedoch einerseits insb aus der Rechenschafts- und Nachweispflicht des *Verantwortlichen* (siehe Art 5 Abs 2 und Art 24 Abs 1 DSGVO),[118] andererseits auch aus Anforderungen an die Datensicherheit (Art 32 DSGVO)[119] ergeben. Daneben existiert in Bezug auf Einwilligungen gem Art 7 Abs 1 DSGVO eine spezifische Nachweispflicht, wonach der *Verantwortliche* die erfolgte Einwilligung der jeweils betroffenen Person nachweisen können muss, was ebenfalls im Ergebnis zu einer Protokollierung führen wird.[120]

Unmittelbar wird eine Protokollierung von Verarbeitungsvorgängen in § 50 DSG normiert, wobei diese Bestimmung in Umsetzung der JI-RL (EU) 2016/680 ergangen ist und daher nur einen (im vorliegenden Kontext nicht erfüllten) eingeschränkten Anwendungsbereich hat.[121]

Bei Protokolldaten handelt es sich nach der Entscheidungspraxis der Datenschutzbehörde idR um personenbezogene Daten.[122] Generell gilt es zu beachten, dass es durch die Vornahme einer Protokollierung auch zu einer eigenen Verarbeitung von Daten kommt,[123] welche (bei Vorliegen personenbezogener Daten) einer Rechtsgrundlage gem Art 6[124] bzw (bei Vorliegen „sensibler" Daten) Art 9 (jeweils iVm Art 5 bzw Art 32 DSGVO) bzw einer entsprechenden Norm im Unionsrecht oder dem nationalen Recht bedarf.

---

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

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

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

[120] Ausführlich dazu *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO Rz 12 ff (Stand 7. 5. 2020, rdb.at)

[121] § 50 DSG ist somit nur auf die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs anwendbar; auf die Protokollierung gem § 13 Abs 2 u 3 DSG wird an dieser Stelle mangels Relevanz nicht eingegangen.

[122] Vgl dazu bspw DSB, Empfehlung vom 31. 01. 2017, DSB-D213.471/0005-DSB/2016.

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

[124] In Frage kommt hier insb Art 6 Abs 1 lit c (Erfüllung einer rechtlichen Verpflichtung; Archivierungspflicht), siehe *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO Rz 13 mwN (Stand 7. 5. 2020, rdb.at) oder Art 6 Abs 1 lit f (IT-Sicherheit) K*astelitz/Hötzendorfer/Tschoh*l in *Knyrim*, DatKomm Art 6 DSGVO Rz 54,wobei lit f gem Art 6 Art 1 letzter Satz DSGVO nicht für die von Behörden in Erfüllung ihrer [hoheitlichen] Aufgaben vorgenommene Verarbeitung gilt; jüngst auch Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung. Orientierungshilfe (2021) Rz 121.

Soweit die Aufzeichnung von Verarbeitungsvorgängen im Einzelfall nicht ausdrücklich gesetzlich angeordnet ist, wird sich die Zulässigkeit (bzw Unzulässigkeit) sowie in der Folge der Umfang der Durchführung einer Protokollierung aus einer **Gesamtbetrachtung** der Datenverarbeitung unter besonderer Beachtung des Grundsatzes der **Verhältnismäßigkeit** ergeben,[125] der sich (neben § 1 Abs 2 letzter Satz DSG)[126] auch in den datenschutzrechtlichen Prinzipien der Datenminimierung (Art 5 Abs 1 lit c DSGVO), der Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO) und der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO)[127] widerspiegelt. Der Grundsatz der Verhältnismäßigkeit erfordert, dass eine Verarbeitung personenbezogener Daten

- einem legitimen Zweck dient (siehe dazu unter 4.6.3),
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen, und
- angemessen, dh verhältnismäßig im engeren Sinne, ist.[128]

Der Grundsatz der Erforderlichkeit besagt, dass eine Verarbeitung personenbezogener Daten nur so weit zulässig ist, als dies für die Erreichung des damit verfolgten Zwecks notwendig ist,[129] es also kein milderes, gleich effektives Mittel gibt. Im Rahmen von Protokollierungsvorgängen wird die Erforderlichkeit einer Protokollierung (und deren Umfang) insb anhand des konkreten **Verarbeitungskontextes**, des **Schutzbedarfs** und der **Risikobewertung** zu beurteilen sein.

In diesem Zusammenhang ist auch Art 5 Abs 1 lit c DSGVO relevant, der die Verarbeitung personenbezogener Daten von der Einhaltung des Grundsatzes der **Datenminimierung** abhängig macht. Laut EuGH geht aus dem Wortlaut dieser Bestimmung hervor, dass mit diesem Prinzip kein allgemeines und absolutes Verbot [der Datenverarbeitung] eingeführt werden soll.[130] Daraus ergibt sich in einer **Gesamtbetrachtung** bei der Speicherung von Protokolldaten also kein Verbot, sondern eine Prüfung auf die Einhaltung des Verhältnismäßigkeitsgrundsatzes im Einzelfall und insbesondere der konkret erforderlichen Datenfelder für die Zweckerreichung der Protokollierung.

Bereits auf Basis des Vorstehenden ist somit die Zulässigkeit einer generellen „Vorratsdatenspeicherung“ durch eine (zeitlich und inhaltlich) uferlose Protokollierung ausgeschlossen.

4.6.1 Was versteht man unter „Protokollierung“?

Bei der Protokollierung in (wie hier) automatisierten Verarbeitungssystemen werden alle oder ausgewählte Aktivitäten (bzw im datenschutzrechtlichen Sinne Verarbeitungsvorgänge iSd Art 4 Z 2 DSGVO,

---

[125] Vgl bereits zum DSG 2000 *Jahnel*, Handbuch Datenschutzrecht [2010] 304 Rz 5/24; siehe auch *Hötzendorfer/Kastelitz* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Datenschutzgesetz § 50 Anm 1.
[126] Dieser lautet: „Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.“.
[127] *Martini* in *Paal/Pauly* (Hrsg), DS-GVO/BDSG[3] (2021) Art 5 Rz 37 (Eingabekontrolle durch Protokollauswertung).
[128] Siehe zB *Bock/Kühne/Mühlhoff/Ost/Rehak/Pohle*, Datenschutz-Folgenabschätzung für die Corona-App, Version 1.6 vom 29. 4. 2020, 61.
[129] Siehe *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 19 mwN. Gem EuGH 16. 12. 2008, C-524/06 handelt es sich beim Begriff der Erforderlichkeit um einen autonomen Begriff des Unionsrechts, der so auszulegen ist, dass er in vollem Umfang dem Ziel der Richtlinie [Anm: DSRL 95/46/EG] als „Vorgängerin“ der DSGVO) entspricht.
[130] EuGH 22. 6. 2021, C-439/19 Rz 104.

wie zB Speicherung, Veränderung, Abfragen, Abgleichen, Löschen)[131] zusammen mit weiteren Metadaten, wie Datum und Zeit des jeweiligen Vorganges („Timestamp"), aufgezeichnet. Ergebnis der Speicherung dieser Protokolldaten sind sogenannte „Protokolle" – auch „Logfiles" oder „Protokolldateien" genannt. Laut dem deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) kann grundsätzlich zwischen zwei Protokollierungsebenen unterschieden werden:[132]

- Protokollierung technischer Systemereignisse auf **Ebene der IT-Infrastruktur („Infrastrukturebene")** zum Zweck der Überwachung der IT-Sicherheit bzw der Datensicherheit[133] (zB Erkennung unbefugter Aktivitäten) sowie der Sicherstellung der ordnungsgemäßen Funktion bzw der Verifizierung und Behebung von Systemfehlern;[134]
- datenschutzrechtlich normierte Protokollierung auf **fachlicher Ebene („Anwendungsebene").**[135] Sie dient insbesondere dem Ziel, eine effiziente Nachprüfbarkeit einzelner Verarbeitungsvorgänge zu ermöglichen, worunter auch die Eigenkontrolle fällt.[136] Zu den protokollierten Vorgängen zählen – abhängig von der konkreten Ausgestaltung – insbesondere Aktivitäten der Nutzer*innen („User") der Anwendungen, wozu sowohl Administrator*innen als auch Endnutzer*innen zählen.

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

4.6.2 Inhalt von Protokolldaten

Da es kaum einheitliche Datenverarbeitungen gibt und sich diese samt der dabei jeweils anfallenden Daten unter anderem hinsichtlich **Verarbeitungskontext**, **Schutzbedarf** und **Risikobewertung** idR unterscheiden werden, sind die Inhalte einer stattfindenden Protokollierung abhängig von der **konkreten Anwendung** und dem verfolgten **Protokollierungszweck**, wobei an dieser Stelle auch auf die obigen Ausführungen zum Grundsatz der Verhältnismäßigkeit zu verweisen ist. So wird im Österr Informati-

[131] Tlw auch als „Transaktionsdaten" bezeichnet.
[132] Vgl BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 1, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_Protokollierung.pdf?__blob=publicationFile&v=2 (abgerufen am 24.08.2023).
[133] Siehe zB *Schallbruch*, Das IT-Sicherheitsgesetz 2.0 – Befugnisse des BSI und Schutz der Bundesverwaltung, CR 2021, 516 (519): „Im Lichte jüngster Cyberangriffe auf Einrichtungen des Bundes […] kommt der Auswertung von Protokolldaten eine besondere Bedeutung zu, um Zeitpunkt des Eindringens, Urheber und Methodik des Angriffs sowie den Umfang der betroffenen Systeme zu ermitteln."
[134] Auch der der Europäische Datenschutzbeauftragte geht von einer Protokollerstellung zur Rekonstruktion von Ereignissen im IT-System aus, EDPS, Leitlinien zum Schutz personenbezogener Daten für die Bereiche IT-Governance und IT-Management der EU-Institutionen (2018) Rz 107, abrufbar unter https://edps.europa.eu/sites/default/files/publication/it_governance_management_de.pdf (abgerufen am 24.08.2023).
[135] In Deutschland auch „Fachanwendungsebene" genannt, siehe BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 1; SDM, Baustein 43 „Protokollieren" (Version 1.0a) 4: „*Fachapplikation*".
[136] Die DSB hat anlässlich ihrer Schwerpunktprüfungen von Krankenanstalten ua die regelmäßige (interne) Nachkontrolle der Zugriffsprotokolle auf Patientendaten verlangt, siehe zB DSB 31. 1. 2017, DSB-D213.471/0005-DSB/2016 und den Überblick bei *Haidinger*, Datenschutz bei Patientendaten, Dako 2016/54.

onssicherheitshandbuch dazu ausgeführt, dass *„Art und Umfang von Protokollierungen von den speziellen Anforderungen des IT-Systems und der darauf befindlichen Applikationen und Daten ab[hängen] und im Einzelfall sorgfältig festzulegen [sind].“*[137]

Beispielhaft muss bei Vorliegen des Protokollierungszwecks „Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ aus **datenschutzrechtlicher** Sicht anhand der Logdateien verifiziert werden können, **wer wann welche** personenbezogenen Daten **wie** verarbeitet hat. So wird im deutschen Standarddatenschutzmodell (SDM) gefordert, dass zur vollständigen Prüfung zumindest die folgenden Protokolldaten erforderlich sind:[138]

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

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

4.6.3 Wozu wird protokolliert?

Als üblicher Zweck der Protokollierung (aus Sicht des Datenschutzrechts und insbesondere der Datensicherheit) ist vor allem die Nachprüfbarkeit der datenschutzrechtlich relevanten Vorgänge anzuführen. Diese Nachprüfbarkeit einzelner Verarbeitungsvorgänge ist dabei Grundvoraussetzung für die Erbringung eines Nachweises der Einhaltung der rechtlichen Datenschutzanforderungen durch den *Verantwortlichen* (Rechenschaftspflicht gem Art 5 Abs 2 DSGVO).[139] Die Kontrollierbarkeit der Ordnungsmäßigkeit der Datenverarbeitung durch Protokollierung ist gleichzeitig auch eine Maßnahme zur Sicherstellung von Informations- und Datensicherheit.[140]

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

Der Zweck der Protokollierung besteht aber auch darin, eine Verarbeitung personenbezogener Daten transparent zu gestalten, betroffenen Personen über die Verarbeitung ihrer Daten auf Nachfrage eine Auskunft erteilen zu können.[141]

---

[137] Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[138] Vgl AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Standard-Datenschutzmodell (SDM), Baustein 43 „Protokollieren“ (Version 1.0a) 2 f (abrufbar unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (abgerufen am 24.08.2023)).
[139] Vgl SDM, Baustein 43 „Protokollieren“ (Version 1.0a) 1.
[140] Siehe Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[141] Vgl *bvitg/gmds/IHE Deutschland*, Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen (2020) 12, abrufbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php (abgerufen am 24.08.2023).

4.6.4 Auswertung von Protokollen

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

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

Mit Bezug auf § 18 Abs 1 letzter Satz E-GovG – wenn auch hier nicht unmittelbar einschlägig – kann aus dem Gesetzeswortlaut und den Materialien[142] abgeleitet werden, dass es dem *Verantwortlichen* und dem *Auftragsverarbeiter* nicht verwehrt ist, den Grundsätzen für die Verarbeitung personenbezogener Daten nachzukommen, worunter zB im Rahmen der Überprüfung der Rechtmäßigkeit der Datenverarbeitung auch die (interne) Auswertung von Protokolldaten fallen wird. Dabei ist jedoch darauf zu achten, dass dabei nur die im Einzelfall relevanten (personenbezogenen) Daten ausgewertet werden dürfen.

Unterstützend kann für diese Ansicht auch die DurchführungsVO (EU) 2015/1502 herangezogen werden, die Folgendes in ihrem Anhang unter Pkt 2.4.4. (Aufbewahrungspflichten) vorsieht:

„1. Die Aufzeichnung und Aufbewahrung einschlägiger Informationen erfolgt mit einem effektiven Aufzeichnungsverwaltungssystem unter Beachtung geltender Vorschriften und bewährter Verfahren auf dem Gebiet des Datenschutzes und der Datenspeicherung.

2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet."[143]

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

[142] ErläutRV 469 BlgNR 27. GP 7.

[143] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, ABl L 235, 7 (18) vom 9. 9. 2015 (Hervorhebung nicht im Original).

Gewährleistung der Revisionssicherheit der Protokolldaten (Manipulationsschutz).[144] Kurz gesprochen: Je höher das (potenzielle) Risiko der Verarbeitung für die betroffenen Personen ist, desto umfangreicher muss der Schutz der Protokolldaten ausfallen.

4.6.5 Wie lange dürfen Protokolle aufbewahrt werden?

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

Mangels ausdrücklicher Anordnung der Speicherdauer durch eine Rechtsnorm (welche aus grundrechtlicher Sicht selbstverständlich in verhältnismäßiger Weise ausgestaltet sein muss) ergibt sich die Aufbewahrungsdauer aus dem Vorliegen der Erforderlichkeit für den jeweiligen Auswertungszweck. Wie lange dieses Kriterium der Erforderlichkeit vorliegt, ist häufig das Ergebnis einer Abwägung, in die neben dem Zweck auch Art und Inhalt der protokollierten Ereignisse und das Ergebnis einer Risikobewertung einfließen können.[145]

In diesem Sinne hat der Gesetzgeber in den Materialien zur Protokollierung gem § 50 DSG nachvollziehbar (und uE verallgemeinerungsfähig) erläutert, dass *„[…] Protokolldaten – wie auch alle anderen personenbezogenen Daten – nur solange in personenbezogener Form aufbewahrt werden [sollten], als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; danach sind die Protokolldaten zu löschen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen. Eine längere Aufbewahrungsdauer muss sich aus besonderen gesetzlichen Vorschriften ergeben.“*[146]

Zumindest personenbezogene Teile von Protokolldaten sind daher nach Zweckerreichung zu löschen bzw zu anonymisieren,[147] sofern auch keine sonstigen gesetzlichen Aufbewahrungsfristen mehr bestehen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen.[148]

Interessant sind die (allerdings im Rahmen eines Art 36 DSGVO-Verfahrens im Bereich einer deutschen Rundfunkanstalt ergangenen) Ausführungen zur Speicherdauer von Logdaten zur Feststellung bzw Abwehr von Cyberattacken.[149] Obwohl deutsche Rundfunkanstalten (jedenfalls zum Zeitpunkt der Entscheidungsfindung) nicht als Betreiber einer kritischen Infrastruktur zu qualifizieren waren, verwies

---

[144] Instruktiv dazu BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz 5.
[145] Siehe dazu Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[146] ErläutRV 1664 BlgNR 25. GP 23.
[147] Beispielsweise können Protokolldaten mit Personenbezug anonymisiert werden, sofern nur noch Metadaten (die keinen Personenbezug aufweisen, Achtung ist daher geboten bei Vorhandensein von IP-Adressen etc) des protokollierten Ereignisses relevant sind, vgl Österr Informationssicherheitshandbuch (Version 4.2.3 vom 31.05.2021) 12.5.2.
[148] Vgl ErläutRV 1664 BlgNR 25. GP 23.
[149] Siehe Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten für das Jahr 2019 Rz 160 ff, abrufbar unter https://www.rundfunkdatenschutz.de/infothek/taetigkeitsbericht-20190.file.html/TB%202019.pdf (abgerufen am 24.08.2023).

der Rundfunkdatenschutzbeauftragte auf die Empfehlung des BSI an Betreiber kritischer Infrastrukturen iSd deutschen BSI-Gesetzes, welche die Speicherung von Logdaten, jedenfalls für Proxy- und Firewall-Logs, für die Dauer von mindestens 90 Tagen vorsieht.[150] Bei zu erwartenden Beschwerden an die Datenschutzbehörde wäre auch die Heranziehung der Fristen in § 24 Abs 4 DSG denkbar. Für die kommende eIDAS 2-VO schlägt ein renommierter Experte eine Aufbewahrungsdauer zwischen zwei Jahren und einem Monat vor, welche aufgrund einer durchgeführten DSFA festzulegen sei.[151]

Das Ergebnis hinsichtlich der Speicherdauer von Protokolldaten muss uE – nicht zuletzt für die interne Umsetzung der Protokollierung und die (externe) Vorlage in einem etwaigen Verfahren vor der Datenschutzbehörde bzw vor Gericht – durch den *Verantwortlichen* niedergeschrieben, also dokumentiert werden. Hierfür ist die Erstellung eines sogenannten Protokollierungskonzepts empfehlenswert.[152]

4.6.6 Exkurs: Auskunftsrecht der betroffenen Personen

Teil der Betroffenenrechte ist das in Art 15 DSGVO normierte Recht auf Auskunft darüber, ob über die (anfragende) betroffene Person personenbezogene Daten verarbeitet werden. Da das Auskunftsrecht (bis auf Rechte und Freiheiten anderer Personen, siehe Art 15 Abs 4 leg cit; beachte auch § 4 Abs 5 und 6 DSG zur Gefährdung gesetzlich übertragener Aufgaben bzw von Geschäfts- oder Betriebsgeheimnissen) nicht weiter eingeschränkt wird, werden davon grds auch (personenbezogene) Protokolldaten erfasst sein, da der EuGH in seiner bisherigen Rsp dieses Betroffenenrecht tendenziell weit ausgelegt hat.[153] Im seinem rezenten Urteil zu C-579/21 erkennt der EuGH, dass die Bereitstellung einer Kopie von Protokolldateien erforderlich sein kann, um den Anforderungen des Auskunftsrechts Genüge zu tun.[154]

Eine Umgehung des (verfassungsrechtlich in § 1 Abs 3 Z 1 DSG und Art 8 Abs 2 GRC festgeschriebenen) Auskunftsrechts durch fehlendes Anlegen von Protokollen, wo dieses gem Art 5 Abs 2 oder Art 32 DSGVO oder sonstige Rechtsgrundlagen erforderlich ist, ist wohl nicht rechtskonform. So hat die DSB auf Grundlage von Art 5 Abs 2 DSGVO entschieden, dass sich ein *Verantwortlicher* der Einhaltung seiner durch die DSGVO auferlegten Pflichten nicht dadurch entziehen kann, indem er ungeeignete technische und organisatorische Maßnahmen trifft, die es ihm ua verunmöglichen, den Anträgen von betroffenen Personen zu entsprechen.[155]

---

[150] BSI, Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen (2021) 12, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf?__blob=publicationFile&v=5 (abgerufen am 24.08.2023).

[151] *Olejnik*, Privacy analysis of European eID Regulation proposal (Pkt 13), https://blog.lukaszolejnik.com/privacy-analysis-of-european-eid-regulation-proposal/ (zuletzt abgerufen am 23.08.2023): "In Article 6a(7): "*The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services."* It should also be defined that the collected information is deleted when not needed: after a time as defined in the DPIA documents prepared. Such a time period may be stipulated in the Regulation itself. It should not exceed two years, possibly even a month?"

[152] Siehe für die erforderlichen Inhalte instruktiv *bvitg/gmds/IHE Deutschland*, Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen (2020), abrufbar unter https://www.gesundheitsdaten-schutz.org/html/protokollierungskonzept.php (abgerufen am 24.08.2023).

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

[154] EuGH C-579/21, ECLI:EU:C:2023:501, Rz 69.

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

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

4.6.7. Umsetzungsstrategie zur Protokollierung im Rahmen der Ausweisplattform

Wie den obenstehenden Ausführungen zu entnehmen ist, sind **Art, Umfang und Dauer der Protokollierung** auf das zur Erfüllung des **Protokollierungszwecks erforderliche Maß** zu beschränken und entsprechende **technische und organisatorische Maßnahmen** zum Schutz von angelegten Protokolldaten zu treffen.

Im System der Ausweisplattform wird im Sinne der obigen Ausführungen im AWP-Backend zum Zweck der Überwachung der grundlegenden Funktionsfähigkeit des Systems einschließlich der IT-Sicherheit und Datensicherheit auf infrastrukturnaher Ebene technische Vorgänge protokolliert, inklusive Angaben, wie etwa Uhrzeit und Ausweistyp (zB Führerschein), zudem im Fehlerfall Referenzen zu Dokumenten, wie etwa „Dokument XY mit ReferenzID Z konnte nicht geladen werden.“. Da die IP-Adressen der Nutzer*innen nicht an die Plattform weitergegeben werden, ist die IP-Adresse betroffener Personen in diesen Protokolldaten nicht vorhanden. Es handelt sich auch demnach hierbei grundsätzlich nicht um personenbezogene Daten.

Beispiele für die Protokollierung infrastrukturnaher Systemereignisse im AWP-Backend (technische Logs):

```
INFO 1 --- [nio-8080-exec-2] c.y.m.m.s.i.u.UserValidityController :
Check validity of user
INFO 1 --- [nio-8080-exec-5] c.y.m.m.s.i.profile.ProfileController :
Profile image request
INFO 1 --- [nio-8080-exec-8] c.y.m.m.s.i.search.SearchController : GET
user cardinfos
INFO 1 --- [nio-8080-exec-9] c.y.m.m.s.i.profile.ProfileController :
Profile request
INFO 1 --- [nio-8080-exec-6] c.y.m.m.s.i.dynamiccard.CardController :
Card request for card type 'abec3d6a-4089-4cdd-964a-4587a0e9279c'
```

Andererseits sieht das der Ausweisplattform zugrundeliegende Software-System auf Anwendungsebene das sog Audit Log vor, das eine Protokollierung der Form, welcher Nutzer*in mit welcher ID mit welcher Device-ID wann welche Aktion ausgelöst hat, ermöglicht. Durch Änderung des sogenannten Log Levels kann dabei in fünf Stufen konfiguriert werden, welche Ereignisse protokolliert werden sollen, von der vollständigen Deaktivierung über eine Einschränkung des Loggings auf schwere Systemfehler bis hin zur Protokollierung so vieler Ereignisse wie möglich. Der *Verantwortliche* hat die Entscheidung getroffen, diese Art der Protokollierung **gänzlich zu deaktivieren**, dh das Feature Audit Log nicht zu nutzen.

Auch Vorgänge des Vorweisens und Überprüfen von digitalen Aus- oder Nachweisen werden im System der Ausweisplattform nicht protokolliert. Dies gilt beispielsweise sowohl beim offline Vorweisen des digitalen Nachweises des Alters als auch bei der Verkehrskontrolle mittels des digitalen Führerscheins.[156]

Im Hinblick auf die rechtlichen Grundlagen der Protokollierung kann im gegebenen Zusammenhang zwischen Art 5 Abs 2 DSGVO (Rechenschaftspflicht), Art 15 Abs 1 lit c DSGVO (Auskunftsrecht der betroffenen Person über Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind) und Art 32 DSGVO (Sicherheit der Verarbeitung) unterschieden werden.

Die Gewährleistung der Sicherheit der Verarbeitung iSd Art 32 DSGVO bzw deren Nachvollziehbarkeit wird durch die Protokollierung grundsätzlich nicht personenbezogener Logs auf infrastrukturnaher Ebene sichergestellt. Sofern personenbezogene Daten davon umfasst wären, ist demnach Art 32 DSGVO die Rechtsgrundlage dafür und der Zweck der Verarbeitung ist die Nachprüfbarkeit der Funktionsweise des Systems, um dessen Sicherheit, insbesondere Integrität und Verfügbarkeit gewährleisten zu können.

Die Rechenschaftspflicht des *Verantwortlichen* (Art 5 Abs 2 DSGVO) wird ohne die Notwendigkeit einer darüberhinausgehenden Protokollierung bei Bedarf insbesondere auch durch Nachweise über den jeweils aktuellen Systemzustand erfüllt.

Ein Zweck und somit eine Rechtsgrundlage der Protokollierung kann insbesondere auch die Pflicht des *Verantwortlichen* gem Art 15 Abs 1 lit c DSGVO zur Auskunft über Empfänger sein, gegenüber denen die personenbezogenen Daten offengelegt worden sind. Da im System der Ausweisplattform keine Übermittlungen personenbezogener Daten durch den *Verantwortlichen* an Dritte erfolgen, besteht diesbezüglich auch keine Notwendigkeit zur Protokollierung.

Auf dem jeweiligen Endgerät in der eAusweise-App, in der eAusweis Check-App sowie in der GWK Check-App erfolgt keine Protokollierung.

Im Folgenden wird kurz auf die einzelnen Verarbeitungstätigkeiten eingegangen, um Besonderheiten iZm der Protokollierung zu erläutern:

Einrichten der eAusweise-App und laden von Aus- bzw. Nachweisen

In diesem Zusammenhang wird Maßgebliches vom System der ID Austria protokolliert (siehe DSFA-Bericht ID Austria).[157]

[156] Zu beachten ist allerdings, dass gemäß § 16b Abs 7 FSG aufseiten des Führerscheinregisters – und somit außerhalb der Systemgrenzen der Ausweisplattform und der Zuständigkeit von dessen Verantwortlichen – eine vollständige Protokollierung aller erfolgten und versuchten Datenabfragen und somit auch von Datenabfragen im Zuge von Verkehrskontrollen, durchgeführt wird, aus der erkennbar ist, welcher Person welche Daten aus dem Führerscheinregister übermittelt wurden, wobei die Protokolldaten für drei Jahre aufbewahrt werden.

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

Widerruf des Gerätezertifikats AWP

Der Widerruf des Gerätezertifikats kann nur durch das ID Austria System ausgelöst werden und ist so nachvollziehbar.

Abmelden von der eAusweise-App

Nachdem eine betroffene Person alle ihre Geräte abgemeldet hat, erwartet sie berechtigterweise, dass in der Ausweisplattform keine Daten darüber mehr vorhanden sind, dass sie in der Vergangenheit die Ausweisplattform genutzt hat. Es wäre in dieser Hinsicht nicht angemessen, ausgerechnet Protokolladen über erfolgte Abmeldungen in der Vergangenheit anzulegen. Bei Auskunftsbegehren gemäß Art 15 DSGVO erfolgt im Fall, dass keine Ausweise bzw Nachweise mehr vorhanden sind, somit eine Leerbeauskunftung.

Überprüfen des Aus- bzw. Nachweises

Zumal diese Verarbeitungstätigkeit offline erfolgt, gibt es keinen Serverzugriff und daher ist eine serverseitige Protokollierung hierbei gar nicht möglich. Auch eine Protokollierung in der eAusweise-App bzw eAusweis-Check-App erfolgt nicht.

4.7 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.

4.8 Rat des Datenschutzbeauftragten und Standpunkt der Betroffenen

Nach Art 35 Abs 2 DSGVO hat der Verantwortliche bei Durchführung einer DSFA den Rat des Datenschutzbeauftragten einzuholen. Ob der Rat des Datenschutzbeauftragten verpflichtend einzuholen ist und inwiefern dem eingeholten Rat des Datenschutzbeauftragten zu folgen ist, wird in der Literatur uneinheitlich kommentiert: *Trieb* geht bspw davon aus, dass die DSGVO keine solche Pflicht statuiert;[158] *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.[159] 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.[160]

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.[161] Die Bestimmung des Abs 9 schafft grundsätzlich die Möglichkeit, die individuelle Meinung einzelner Betroffener in Erfahrung zu bringen.[162] 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 Stellte vertritt.[163] Auch diese Regelung lässt in mehrfacher Hinsicht Deutungsspielräume offen.[164] 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.[165] Eine bedingungslose Verpflichtung für Verantwortliche zur Einholung wird auf Basis dieser Bestimmung nicht unterstellt werden können;[166] die jeweilige Vorgehensweise ist jedoch zu dokumentieren bzw zu begründen.[167]

---

[158] Vgl *Trieb*, in *Knyrim*, DatKomm Art 35 Rz 124.
[159] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 18.
[160] So die *Art-29-Datenschutzgruppe*, WP 243 rev. 01, 17 unter Hinweis auf Art 24 Abs 1 DSGVO.
[161] Siehe hierzu auch *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01 (2017) 28 f.
[162] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.
[163] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 134; vgl hierzu auch *Martin/Friedewald/Schierung/Mester/Hallinan/Jensen*, Datenschutz-Folgenabschätzung nach Art 35 DSGVO, Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe (2020) 38 ff.
[164] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.
[165] 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.
[166] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 131.
[167] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 58.

Im vorliegenden Fall hatte sich das BMF bereits zu Beginn des Projekts digitaler Führerschein und Ausweisplattform (2021) dazu entschieden, stellvertretend für die Betroffenen aktiv auf die einschlägigen Interessenvertretungen ARBÖ, ÖAMTC sowie VCÖ zuzugehen, um diese in die Entwicklung entsprechend einzubeziehen und die Gelegenheit zu bieten, die Standpunkte und sonstigen Belange der vertretenen Betroffenen in den Fokus der Aufmerksamkeit zu lenken, um diese im Projekt bestmöglich zu berücksichtigen und soweit wie möglich miteinfließen zu lassen. Im Lichte der aktuellen Nutzungsmöglichkeiten fanden insbesondere mit dem ÖAMTC mehrere Abstimmungstermine mit fachlichem und technischem Austausch statt.

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).

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,[168] 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.[169] 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.[170] 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.

---

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

[169] 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.

[170] 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.[171]

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 Aus- oder Nachweise 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.[172]

[171] https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf (abgerufen am 24.08.2023).
[172] 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.[173] Darüber hinaus wurde Anleihe am Risk Assessment-Leitfaden des deutschen Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom),[174] sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Fraunhofer-Institutes für System- und Innovationsforschung genommen.[175]

Der European Data Protection Supervisor (EDPS) sieht grundsätzliche keine spezifische Methode zur Durchführung einer DSFA vor, sondern erachtet jede Vorgehensweise für zulässig, die im Einklang mit den Vorschriften der DSGVO und den Leitlinien der Artikel-29-Datenschutzgruppe steht.[176]

Die Artikel-29-Datenschutzgruppe empfiehlt für die Durchführung einer Risikobeurteilung, mit Verweis auf Art 35 Abs 7 sowie ErwGr 84 und 90 der DSGVO, insb[177]

- 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.[178]

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.[179]

In den methodischen Ausführungen des Fraunhofer-Instituts werden für die generelle Erfassung eines Risikoszenarios wiederum die folgenden übergeordneten Fragen aufgeworfen:[180]

- 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?

---

[173] https://www.iso.org/standard/65694.html (abgerufen am 24.08.2023).
[174] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung, https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf (2017) (abgerufen am 24.08.2023).
[175] 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.
[176] Vgl *European Data Protection Supervisor (EDPS)*, Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 6.
[177] 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.
[178] Siehe Art 35 Abs 7 lit d sowie ErwGr 84 und 90 DSGVO.
[179] Vgl ErwGr 83 DSGVO.
[180] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 43.

– Welche Abhilfemaßnahmen sind bereits implementiert bzw geplant?[181]

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:[182]

– **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 „[...] a*nhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt“*.[183]

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

[181] Zudem kann ergänzt werden, welche zusätzlichen Maßnahmen sich bestimmen lassen um die identifizierten Risiken zu mitigieren.
[182] 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.
[183] Vgl ErwGr 76 DSGVO.

Risikobeurteilung (Template)

1) Risikoidentifikation	**Risikobeschreibung**
	Beschreibung und kurze deskriptive Erläuterung des Szenarios, Nennung beteiligter Akteure und Personen,[184] Nennung verarbeiteter Datenkategorien
	Risikoquelle
	Was sind die auslösenden Elemente für den Schadenseintritt? **Handelt es sich um eine menschliche oder technische Risikoquelle?** **Interne menschliche Quellen:** Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar **Externe menschliche Quellen:** 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 **Interne / externe technische Quellen:** Systemfehler (Software/Hardware) führen zu Verlust, Veränderung; Nichtverfügbarkeit oder missbräuchlicher Verwendung personenbezogener Daten **Bsp Risikoquelle:** • Interne Mitarbeiter*innen, • Externe Mitarbeiter*innen, • Betroffene, • Sonstige Dritte, • Softwarefehler, • Hardwaredefekt (physikalisch), • Umwelteinflüsse (Naturgewalt), • Cyberkriminelle (Hacker/Schadsoftware), • staatliche Institutionen (Nachrichtendienste, Strafverfolgung), • Geschäftsführung.
	Risikoursache
	Was löst den Eintritt des Schadens aus und führt zur „Verwirklichung des Risikos“? Dies dürfte regelmäßig in der Nichteinhaltung der Datenschutzgrundsätze (Art 5 Abs 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art 12 bis 22 DSGVO) oder

[184] 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 23.08.2023) 30 f.

	anderer Verstöße gegen die DSGVO (wie zB einem ungerechtfertigten Datentransfer ins Ausland) liegen.[185] **Bsp Ursachen:** • Unbefugte oder unrechtmäßige Verarbeitung, • Verarbeitung wider Treu und Glauben, • Für die Betroffenen intransparente Verarbeitung, • Unbefugte Offenlegung von und Zugang zu Daten, • Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten, • Verweigerung der Betroffenenrechte, • Verwendung der Daten durch die Verantwortlichen zu inkompatiblen Zwecken, • Verarbeitung nicht vorhergesehener Daten, • Verarbeitung nicht richtiger Daten, • Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler), • Verarbeitung über die Speicherfrist hinaus, • Die Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt (zB weil diese illegitim ist/einer Rechtsgrundlage entbehrt), • Verarbeitung wider den Zweckbindungsgrundsatz.
	Möglicher Schaden für die betroffenen Personen
	Welche Schäden und Beeinträchtigungen von Rechten und Freiheiten der Betroffenen lassen sich feststellen? Handelt es sich um einen physischen, materiellen oder immateriellen Schaden?[186] **Bsp physische Schäden:** körperliche Schäden (zB durch falsche medizinische Behandlung); wenn Verstöße gegen die Vertraulichkeit Gewaltverbrechen, einschließlich Stalking, Vorschub leisten; psychologische Schäden (wie zB Angstzustände oder Depressionen) **Bsp materielle Schäden:** wirtschaftliche Schäden, berufliche Nachteile (wie zB entgangene Einstellung oder Beförderung, Jobverlust), Beschneidung staatlicher Leistungen (wie zB Arbeitslosengeld, Sozialhilfe), Diskriminierung (zB bei Versicherungsabschlüssen oder Wohnungssuche), ungerechtfertigte Gebühren oder Bußgelder usw **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)

[185] Siehe hierzu auch *Martin et al*, Datenschutz-Folgenabschätzung 38 ff.
[186] *Friedewald et al*, Datenschutz-Folgenabschätzung 30 f.

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

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

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

Der Prozess der datenschutzrechtlichen Risikobeurteilung erfolgt im vorliegenden Fall somit anhand der folgenden 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.[187] 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.[188] Im Zuge der Risikobeurteilung sind

[187] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 38 ff.

[188] 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 eruieren.[189] Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annahmen zur angemessenen Einstufung des identifizierten Risikoszenarios.[190]

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit[191]

Wert	**Beschreibung**
Vernachlässigbar	Es erscheint nicht sehr wahrscheinlich, dass eine Bedrohung eintritt (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät 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 Papierdokumenten 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 Papierdokumenten aus einer öffentlich zugänglichen Lobby).

Tabelle 2: Risikoausprägungen für Schadensausmaß[192]

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

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in einer Risikomatrix verortet. Der Risikograd ist methodisch definiert als das Produkt von Eintrittswahrscheinlichkeit und Schadensausmaß.[193] 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,[194] wie in der nachfolgenden Risikomatrix dargestellt.

[189] Vgl ErwGr 75 und 76 DSGVO.
[190] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 ff; vgl *CNIL*, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.
[191] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 30 f.
[192] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 f.
[193] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 8 (9).
[194] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46; vgl hierzu weiterführend auch *Friedewald et al*, Datenschutz-Folgenabschätzung 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.[195]

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.[196] 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.[197]

Die in Art 35 Abs 7 lit d DSGVO genannte „Bewältigung" wird gemeinhin auch als „Reduktion" bzw „Eindämmung" verstanden.[198] Durch die Maßnahmen sollten zumindest alle als „hoch" bewerteten Risiken so weit reduziert werden, dass sie nur noch als „normal" einzustufen sind.[199] Dabei ist es nicht zwangsläufig notwendig, zusätzliche Maßnahmen zu implementieren; mitunter kann es auch sinnvoller sein, bestehende Maßnahmen zu stärken.[200]

[195] Vgl *Friedewald et al*, Datenschutz-Folgenabschätzung 31.
[196] Siehe Art 35 Abs 7 lit d DSGVO; vgl *Martin et al*, Datenschutz-Folgenabschätzung 38.
[197] Vgl ErwGr 78 DSGVO.
[198] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46.
[199] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 47.
[200] 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:[201]

- 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.[202] Die verschiedenen Maßnahmen, Garantien und Verfahren sollen letztlich den Schutz personenbezogener Daten sicherstellen und die Einhaltung der Bestimmungen dieser Verordnung nachweisen.[203]

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*.[204] 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.[205] 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.[206]

---

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

[202] 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.

[203] Vgl ErwGr 90 DSGVO.

[204] 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.

[205] 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.

[206] 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.[207] 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/Irrütmliche Auslösung von Datenverarbeitungen in der eAusweise-App

1) Risikoidentifikation	**Risikobeschreibung**
	Die prüfende Person möchte zwar weder die eAusweise-App noch digitale Aus- und Nachweise nutzen, installiert und verwendet diese aber dennoch. Aufgrund der irrigen Annahme, dies sei für die Durchführung einer Prüfung notwendig, meldet sie sich an der ID-Austria an und lädt einen Aus- oder Nachweis.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Entscheidungsträger*innen des *Verantwortlichen* • Interne Mitarbeiter*innen • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache
	• Derartig ausgestaltete eAusweise-App, dass der Eindruck entstehen kann, dass die Durchführung einer Prüfung einer Anmeldung einer ID-Austria oder anderweitigen Verarbeitung von daten der prüfenden Person bedarf. • Unpräzise oder fehlende Kommunikation durch den *Verantwortlichen* oder andere zuständige Stellen, dass der analoge Ausweis weiterhin uneingeschränkt genutzt werden kann • Größere Zahl von Privaten, insbesondere Unternehmen, deren Verhalten zu entsprechenden Drucksituationen führt
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden:

[207] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 113.

	• 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 der darauf basierenden Funktionen 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**
	Maximal (4) Kommentar: Auch irreführende Ausgestaltungsvarianten der Applikation sind denkbar.	Wesentlich (3) Kommentar: Wenn sich dieses Risiko materialisiert, wird die betroffene Person unfreiwillig dem Potenzial ausgesetzt, dass sich alle folgenden Risiken materialisieren und somit auch das schwerwiegendste dieser (auch funktionsbezogenen) Risiken. Dies jedoch nur mittelbar als Folgeschaden.	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Stringente Außenkommunikation hinsichtlich Nutzungsmöglichkeiten des Prüfprozesses • Transparente Gestaltung der eAusweise-App, sodass es eindeutig ist, dass eine Prüfung ohne Registrierung/Anmeldung möglich ist. • Die eAusweise-App kann nach einer erstmaligen Einrichtung ohne ID Austria Anmeldung für eine Prüfung verwendet werden. Eine ID Austria Anmeldung wird ausschließlich zum Zweck des aktiven Hinzufügens eines neuen Aus- oder Nachweises ausgelöst. Der Zweck dieser Datenverarbeitung ist klar ersichtlich.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Eingeschränkt (2) Kommentar: Abmeldung und damit die Vermeidung von Folgeschäden jederzeit möglich.	Normal (4)

5.2.2 Unfreiwillige Nutzung biometrischer Authentifizierungsfunktionen

1) Risikoidentifikation	**Risikobeschreibung**
	Die eAusweise-App setzt zwingend das Vorhandensein und die Verwendung einer biometrischen Authentifizierungsfunktion auf dem Endgerät der betroffenen Person voraus (Fingerabdruck-Sensor oder Face ID). Das bedeutet, auf dem Endgerät der betroffenen Person werden zum Zweck der Authentifizierung biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) und somit sensible Daten iSv Art 9 Abs 1 DSGVO verarbeitet. [208] Insbesondere falls die Nutzung von digitalen Ausweisen und Nachweisen künftig weite Verbreitung finden sollte, kann es zu Formen sozialen Drucks oder faktischen Zwangs zur Nutzung der eAusweise-App bzw der darauf basierenden Funktionen kommen. Personen, die die Verwendung biometrischer Daten zu Authentifizierungszwecken auf ihrem mobilen Endgerät ablehnen, könnten auf diese Weise in die Situation kommen, dass sie die biometrische Authentifizierungsfunktionen gegen ihren Willen trotzdem nutzen, um die eAusweise-App verwenden zu können und dadurch Nachteile zu vermeiden. Dieses Risiko kann auch ohne eAusweise-App eintreten, aber die eAusweise-App kann sich diesbezüglich risikoerhöhend auswirken, nämlich dann, wenn die betroffene Person nur deswegen begonnen hat, die Biometriefunktion des Endgeräts zu nutzen, um die eAusweise-App zu nutzen. Für diese Personen bewirkt die eAusweise-App, dass überhaupt erst ein Risiko für ihre biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) entsteht.
	Risikoquelle
	Externe menschliche Quelle: • Sonstige Dritte (insb Anbieter*innen von Drittdiensten) **Interne technische Quelle:** • Softwarearchitektur (Mangel an alternativen Authentifizierungsformen)
	Risikoursache
	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu entsprechendem Druck zur Nutzung der eAusweise-App. • Heranziehen von Biometrie zur Authentifizierung • Einschränkung der informationellen Selbstbestimmung
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden

[208] Die biometrischen Daten werden ausschließlich gemäß den geltenden technischen Standards der Hersteller auf den Geräten der Benutzer*innen verarbeitet. Eine Verarbeitung dieser Daten durch den Betreiber der Ausweisplattform erfolgt zu keinem Zeitpunkt.

	• Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung von Biometrie verbunden sind, da die betroffene Person diese eigentlich gar nicht verwenden würde, wenn sie sich frei entscheiden hätte können **Immaterielle Schäden:** • Verarbeitung personenbezogener Daten gegen den Willen der betroffenen Person • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer unrechtmäßigen Datenverarbeitung. • Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung von Biometrie 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**
	Maximal (4)	Wesentlich (3) Kommentar: Wenn sich dieses Risiko materialisiert, wird die betroffene Person unfreiwillig dem Potenzial ausgesetzt, dass sich das biometriebezogene Risiko 5.2.6 materialisiert.	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Physische Ausweise und Nachweise können weiterhin diskriminierungsfrei in allen Lebenslagen verwendet werden • Stringente Außenkommunikation hinsichtlich Nutzungsmöglichkeiten physischer Ausweise und Nachweise

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Wesentlich (3)	Normal (9)

5.2.3 Protokollierung zu vieler personenbezogener Daten

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass im Zuge der Verwendung der eAusweise-App auf der Ebene der Ausweisplattform 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.
	Risikoquelle
	Interne technische Quellen: • Softwarearchitektur, welche etwa standardmäßig bestimmte Daten protokolliert • Softwarekonfiguration
	Risikoursache
	• 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
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen), berufliche Nachteile • Finanzieller Verlust, etwa da die temporäre Abnahme eines Führerscheins bekannt wird **Immaterielle Schäden** • Rufschädigung • Verletzung der Privatsphäre • wirtschaftliche oder gesellschaftliche Nachteile • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Das Vorweisen von Nachweisen findet offline statt (außer bei einer Prüfung durch	Normal (6)

		Exekutivorgane). 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.	

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Aus- oder Nachweises findet offline statt (Vorbehaltlich der Prüfung durch Exekutivorgane). 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. • Das Protokollierungskonzept wurde so gestaltet, dass die oben genannten Risikoursachen nicht zutreffen. • Backup-Konzept • Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (zB eingeschränkte Zugriffsrechte entsprechend Need-To-Know-Prinzip; Zugriffe nur nach Vier-Augen-Prinzip) • Gewährleistung der Revisionssicherheit der Protokolle: Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden. Protokolldaten sollten nicht auf den Produktivsystemen, sondern auf eigens hierfür vorgehaltenen zugriffsbeschränkten zentralen Protokollservern gespeichert werden. Die zu protokollierenden Ereignisse sollten in Echtzeit über ein sicheres Protokoll auf die Protokollserver übertragen werden. • Protokollierung des Zugriffs auf Protokolldaten • Schulung der involvierten Personen; klare Kommunikation und Aufklärung über die Einschränkung der Protokollierung und die Konsequenzen eines dienstlich nicht erforderlichen Zugriffs auf Protokolldaten (etwa Disziplinarmaßnahmen bzw Strafen)	

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

5.2.4 Missbräuchliche Verwendung von Protokolldaten

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass Protokolldaten auf der Ebene der Ausweisplattform offengelegt bzw zweckwidrig verarbeitet werden und deshalb insbesondere bekannt wird, an welchen Stellen Betroffene ihren digitalen Aus- oder Nachweis verwendet haben.
	Risikoquelle
	Interne/externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) • staatliche Institutionen (Nachrichtendienste, Strafverfolgung) **Interne / externe technische Quellen:** • Softwarefehler (zB mangelhafte Verschlüsselung, offene Schnittstellen)
	Risikoursache
	• Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • 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
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • 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 Aus- oder Nachweises findet offline statt (außer bei einer Prüfung durch Exekutivorgane). 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.	Mittel (9)

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Aus- oder Nachweises findet offline statt (Vorbehaltlich der Prüfung durch Exekutivorgane). 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. • Protokollierungskonzept: Die Protokollierung ist auf das technisch notwendige Minimum beschränkt; entsprechend reduziert ist auch das mit Protokolldaten verbundene potenzielle Schadensausmaß n. • Bereitstellung einer sicheren Umgebung für Protokolldaten, auf welche (ausschließlich) berechtigte Nutzer*innen zugreifen können • Backup-Konzept • Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (zB eingeschränkte Zugriffsrechte entsprechend Need-To-Know-Prinzip; Zugriffe nur nach Vier-Augen-Prinzip) • Gewährleistung der Revisionssicherheit der Protokolle: Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden. Protokolldaten sollten nicht auf den Produktivsystemen, sondern auf eigens hierfür vorgehaltenen zugriffsbeschränkten zentralen Protokollservern gespeichert werden. Die zu protokollierenden Ereignisse sollten in Echtzeit über ein sicheres Protokoll auf die Protokollserver übertragen werden.	

	• Schulung der involvierten Personen; Klare Kommunikation und Aufklärung über die Konsequenzen missbräuchlicher Verwendung (etwa Disziplinarmaßnahmen bzw Strafen)

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)

5.2.5 Nichtverfügbarkeit des Systems

1) Risikoidentifikation	**Risikobeschreibung**
	Das System steht der Nutzer*in nicht zur Verfügung und sie kann daher ihren digitalen Nachweis nicht vorweisen. 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, können sich je nach Szenario möglicherweise verwaltungsrechtliche Folgen oder Nachteile im Rechtsverkehr ergeben.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Betroffene • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) **Interne / externe technische Quellen:** • Softwarefehler • Endgerät • Hardwaredefekt (physikalisch) **Sonstige Quellen:** • Umwelteinflüsse (Naturgewalt)
	Risikoursache
	Der Eintritt des Risikostritt in diesem Bereich tritt aufgrund des Ausfalls der Ausweisplattform auf, weshalb Nach- bzw. Ausweise nicht geladen werden können.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • 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 **Immaterielle Schäden:** • 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
	Eingeschränkt (2) Kommentar: Der Ausfall der Ausweisplattform ist nur während des Ladens des Nach- bzw. Ausweises relevant und nicht während Nachweisvorgängen.	Wesentlich (3) Kommentar: Das Risiko manifestiert sich erst mittelbar.	Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	• Physische Ausweise und Nachweise 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 von digitalen Ausweisen und Nachweisen als moderne Inklusionsvariante und somit gleichsam als Gegenteil eines Einschränkungsinstruments konzipiert ist. • Das Vorweisen und Prüfen von digitalen Ausweisen und Nachweisen ist prinzipiell als Offline-Prozess konzipiert und damit nicht von der Verfügbarkeit von Serverarchitektur abhängig.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Vernachlässigbar (1)	Eingeschränkt (2) Kommentar: Abhilfe durch physischen Ausweis möglich	Niedrig (2)

5.2.6 Unbefugte Verarbeitung biometrischer Daten

1) Risikoidentifikation	**Risikobeschreibung**
	Auf dem Endgerät der betroffenen Person werden zum Zweck der Authentifizierung biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) und somit sensible Daten iSv Art 9 Abs 1 DSGVO verarbeitet. Es besteht das Risiko, dass biometrische Daten (Fingerabdruck, Face-ID) das Endgerät der betroffenen Person verlassen und an Dritte gelangen. Die zur Verarbeitung der biometrischen Daten verwendete Software und Hardware steht nicht unter der Kontrolle des *Verantwortlichen*; hier verlassen sich sowohl das BMF als auch die Nutzer*innen darauf, dass Hardware- und Softwarehersteller die Biometriefunktion angemessen absichern, ohne dass diese in der Rolle des *Auftragsverarbeiters* sind. Dieses Risiko kann auch ohne eAusweise-App eintreten, aber die eAusweise-App kann sich diesbezüglich risikoerhöhend auswirken, nämlich dann, wenn die betroffene Person nur deswegen begonnen hat, die Biometriefunktion des Endgeräts zu nutzen, um ID Austria und in weiterer Folge die eAusweise-App zu nutzen. Für diese Personen bewirkten die eAusweise-App bzw ID Austria, dass überhaupt erst ein Risiko für ihre biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) entsteht.
	Risikoquelle
	Interne / Externe Menschliche Quellen: • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) **Interne / externe technische Quellen** • Softwarefehler • Hardwaredefekt (physikalisch)
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Finanzieller Verlust **Immaterielle Schäden:** • Schädigung der Privatsphäre • Unumkehrbarer Verlust der Kontrolle über die eigenen biometrischen Daten • Identitätsdiebstahl oder -betrug

	• Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Maximal (4) Kommentar: Aufgrund der Unveränderlichkeit der biometrischen Merkmale des Menschen, ist ein solcher Schaden idR dauerhaft, dh nicht wiedergutzumachen.	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Weder die eAusweise-App noch die serverseitige Plattform haben auf die biometrischen Daten der Nutzer*innen Zugriff. Es wird somit auch keine zentrale Datenbank mit biometrischen Merkmalen aller Nutzer*innen der eAusweise-App geführt. • Verarbeitung biometrischer Daten auf gesichertem und abgesondertem Modul am Endgerät • Verarbeitung biometrischer Daten erfolgt ausschließlich auf dem Endgerät • Exklusive Einbindung von Endgeräten, welche über entsprechende Sicherheitsmaßnahmen verfügen • In der Regel werden bei Android-Geräten Minutien der Fingerabdrücke gespeichert und nicht der volle Fingerabdruck.[209] Bei iOS-Geräten wird allgemein nur eine mathematische Darstellung der Fingerabdrücke abgespeichert. Ein tatsächlicher Fingerabdruck kann aus diesen gespeicherten Daten nicht hergeleitet werden.[210] • Außerdem ist in diesem Zusammenhang festzuhalten, dass die Verwendung von digitalen Ausweisen und Nachweisen durch die Bürger*in auf freiwilliger Basis geschieht. Sollten Vorbehalte gegenüber dem Einsatz biometrischer Merkmale existieren, stehen nach wie vor physische Ausweise und Nachweise zur Verfügung.

[209] *Garg/Yadav/Kamal*, Android Notes using Finger Print Authentication, IJSR, Volume 10 Issue 5, May 2021, DOI: 10.21275/SR21405101230, Seite 175.
[210] https://support.apple.com/de-de/HT204587 (abgerufen am 23.08.2023).

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Wesentlich (3) Kommentar: Wenn keine Daten über vollständige Fingerabdrücke als solche verarbeitet werden, sondern nur daraus abgeleitete Daten, kann der oben beschriebene maximale Schaden nicht eintreten.	Normal (6)

5.2.7 Durchbrechung der Unbeobachtbarkeit

1) Risikoidentifikation	**Risikobeschreibung**
	Das Vorweisen digitaler Ausweise und Nachweise (Funktionen) ist bewusst so konzipiert, dass dabei keine Serverzugriffe (außer bei Prüfungen durch Exekutivorgane) notwendig sind („Offline-Use-Case“). Äquivalent zum Vorweisen eines physischen Ausweises oder Nachweises soll dadurch jegliches Sammeln von Daten darüber, wann sich wer wem gegenüber ausgewiesen bzw einen Nachweis erbracht hat, von vornherein ausgeschlossen werden (Schutzziel der Unbeobachtbarkeit). Diesbezüglich besteht das Risiko, dass die Implementierung diesem Ziel nicht gerecht wird, und letztlich doch eine Möglichkeit gefunden wird, insbesondere über Umwege und/oder mittelbar, solche Daten – allenfalls zumindest theoretisch – zu erheben. Eine solche Möglichkeit wäre zB eine falsche Implementierung der Zertifikatsperrliste (Certificate Revocation List, CRL).
	Risikoquelle
	Interne / Externe menschliche Risikoquellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) • staatliche Institutionen (Nachrichtendienste, Strafverfolgung) **Interne / Externe technische Quellen** • Softwarearchitektur • Softwarekonfiguration • Softwarefehler
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Protokollierung
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • wirtschaftliche oder gesellschaftliche Nachteile • Verletzung der Privatsphäre

	• Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Maximal (4) Kommentar: Hier sind alle Funktionen zu betrachten	Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Die Zertifikatsperrliste (Certificate Revocation List, CRL) wurde so implementiert, dass die Liste vollständig auf das Endgerät der überprüfenden Person geladen wird, und die Zertifikatsprüfung anhand der Liste dann auf dem Endgerät erfolgt. Auf diese Weise wird verhindert, dass die Information, welches (und somit wessen) Zertifikat gerade geprüft wird, nicht auf den Server gelangt. • Die diesbezüglich zum Einsatz gebrachten Sicherheitstechniken und -prozesse der BRZ GmbH entsprechen dem Stand der Technik und werden laufend an die aktuellen Bedrohungsszenarien angepasst. • Die BRZ GmbH ist nach den in diesem Zusammenhang relevanten und international anerkannten Standards ISO 22301 sowie ISO9001 zertifiziert.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Maximal (4)	Normal (8)

5.2.8 Auslesen von Ausweis- oder Nachweisdaten durch eine unautorisierte App und unbefugtes Weiterverarbeiten dieser Daten

1) Risikoidentifikation	**Risikobeschreibung**
	Ohne, dass die betroffene Person es bemerkt, ohne, dass ihr die Tragweite dessen bewusst wird oder ohne, dass sie (zB aufgrund einer Drucksituation) etwas dagegen unternehmen kann, verwendet eine dritte Person, der die betroffene Person ihren digitalen Ausweis oder Nachweis vorzeigt, nicht die eAusweise-App und auch nicht die eAusweis Check-App, sondern eine andere App, die dazu in der Lage ist, erfolgreich mit der eAusweise-App zu kommunizieren. Es gelingt dieser Person, die Ausweis- oder Nachweisdaten mit dieser App auszulesen und ggf zu speichern bzw unbefugt weiterzuverarbeiten.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte • Cyberkriminelle
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Druck auf die betroffene Person • Leichtgläubigkeit der betroffenen Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit dem digitalen Ausweis • 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
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • gesellschaftliche Nachteile • Verletzung der Privatsphäre • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Wesentlich (3)	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	• Vorsätzliche missbräuchliche Verwendung ist durch entsprechende strafrechtliche sowie verwaltungsstrafrechtliche Tatbestände strafbewehrt. • *Geplante* Maßnahme: Implementierung der Steuerung der Auslesbarkeits- bzw Überprüfungsmöglichkeiten durch Key Attestation Mechanisms

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Wesentlich (3)	Normal (9)

5.2.9 Unbewusste oder irrtümliche Datenherausgabe

1) Risikoidentifikation	**Risikobeschreibung**
	Eine betroffene Person gibt personenbezogene Daten über die eAusweise-App an einen *Dritten* weiter, ohne dass ihr das (zur Gänze) bewusst ist. Das kann irrtümlich erfolgen oder von den Daten empfangenden Dritten sogar bewusst herbeigeführt werden, denn diese haben einen Anreiz, an die hochqualitativen hoheitlichen Daten heranzukommen.
	Risikoquelle
	Interne / Externe menschliche und strukturelle Risikoquelle: • Betroffene • Sonstige Dritte
	Risikoursache
	• Unaufmerksamkeit der betroffenen Person • Unwissen der betroffenen Person • Körperliche Einschränkungen der betroffenen Person (zB Sehschwäche, motorische Einschränkungen in Bezug auf die Touch-Bedienung) • Leseschwäche der betroffenen Person • Ignoranz/Ungeduld der betroffenen Person • Intransparente Verarbeitung • Bewusste Herbeiführung des Irrtums/der unbewussten Handlung • Unübersichtliches grafisches Userinterface (GUI) bzw mangelhafte Usability der eAusweise-App • Unbeabsichtigtes Handeln: Besonders Menschen, die im Umgang mit digitalen Diensten nicht besonders geübt oder körperlich eingeschränkt sind, können rasch Vorgänge auslösen, die ihnen nicht bewusst sind und die sie eigentlich nicht wollen. Zudem ist empirisch erwiesen, dass datenschutzrechtliche Informationstexte idR kaum gelesen werden, sondern die Betroffenen einfach auf „weiter“ klicken, um möglichst rasch ans Ziel zu gelangen.[211]
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust

[211] Siehe hierzu grundlegend zB die Studie von *McDonald/Cranor*, The Cost of Reading Privacy Policies, in: Journal of Law and Policy for the Information Society, (2008) Vol 4, No. 3, 543-568; vgl auch *Rothmann/Buchner*, Der typische Facebook-Nutzer zwischen Recht und Realität, in: DuD (2018) Volume 42 (6), 342-346.

	Immaterielle Schäden • Rufschädigung • gesellschaftliche Nachteile • Verletzung der Privatsphäre • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Wesentlich (3)	Normal (9)

3) Maßnahmen	**Bestehende Maßnahmen**
	• In den meisten Fällen werden Risiken betreffend die Datenherausgabe dadurch entschärft, dass die Datenherausgabe nur mit Mitwirkung der betroffenen Person möglich ist. Hier geht es um jene Fälle, in denen die betroffene Person unbewusst oder irrtümlich anders agiert, als sie bei vollem Bewusstsein über die Konsequenzen ihres Handelns agieren würde. • Transparente, leicht erreichbare Informationserteilung durch den *Verantwortlichen* • Stringente FAQs • Übersichtliches User Interface

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

5.2.10 Weiterverarbeiten der Ausweis- oder Nachweisdaten durch die überprüfende Person

1) Risikoidentifikation	**Risikobeschreibung**
	Der derzeitige Funktionsumfang der Überprüfungsfunktion der eAusweise-App sowie der anonymen Überprüfungs-App erlaubt es nicht, die bei der Ausweis- bzw Nachweisprüfung ausgelesenen Daten zu speichern oder anderweitig weiterzuverarbeiten. Sollte jedoch der Überprüfende einen Weg finden, die ausgelesenen Daten auf seinem Endgerät zu speichern oder anderweitig weiterzuverarbeiten – und eine einfache, wenn auch nicht sehr praktikable Möglichkeit dazu ist das Erstellen von Screenshots –, oder eine offizielle Möglichkeit der Ausweis bzw Nachweisüberprüfung geschaffen werden, die eine Weiterverarbeitung der personenbezogenen Daten nach der Überprüfung ausdrücklich ermöglicht, dann würde das Vorzeigen eines digitalen Ausweises oder Nachweises Datenspuren hinterlassen und zu einer potenziellen Weiterverbreitung personenbezogener Daten der betroffenen Person führen, wie dies beim Vorzeigen eines physischen Ausweises oder Nachweises nicht der Fall ist. Eine solche bequeme Weiterverarbeitungsmöglichkeit der Daten könnte wiederum dazu führen, dass Private häufiger als bisher einen Nachweis der Identität von Betroffenen verlangen und Daten von Betroffenen erheben und speichern bzw weiterverarbeiten, weil dies mit einem digitalen Ausweis bzw Nachweis elektronisch für beide Seiten deutlich bequemer ist als bisher. Hinsichtlich der Risikoerhöhung ist anzumerken, dass auch beim Vorweisen physischer Ausweise und Nachweise ein Weiterverarbeiten der personenbezogenen Daten durch die überprüfende Person nicht ausgeschlossen ist. Wesentliche Unterschiede bestehen aber darin, dass das Vorliegen digitaler Daten das Weiterverarbeiten wesentlich erleichtert und dass ein von der betroffenen Person unbemerktes Erheben der Daten aus dem physischen Ausweis oder Nachweis nahezu ausgeschlossen ist, wenn diese ihn nicht aus der Hand gibt, ein Weiterverarbeiten der Daten im Zuge des Überprüfungsvorgangs beim digitalen Ausweis oder Nachweis hingegen sehr leicht vor der betroffenen Person verborgen werden kann.
	Risikoquelle
	Externe menschliche Quellen: • Betroffene • Sonstige Dritte
	Risikoursache
	• Bequeme Austausch- und Weiterverarbeitungsmöglichkeit der Ausweisdaten • Druck auf die betroffene Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit dem digitalen Ausweis • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Verarbeitung entgegen den Zweckbindungsgrundsatz

	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • gesellschaftliche Nachteile • Verletzung der Privatsphäre • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte • Verlust der Kontrolle durch betroffene Personen • Beeinträchtigung der Informationellen Selbstbestimmung

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Wesentlich (3) Kommentar: Denkbar erscheint auch eine Profilbildung	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	• In der Überprüfungsfunktion der eAusweise-App sowie in der anonymen Überprüfungs-App ist die Weiterverarbeitung von Ausweis- und Nachweisdaten nicht vorgesehen.

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

5.2.11 Rechtswidrige Verarbeitung durch Zugriffsbefugte

1) Risikoidentifikation	**Risikobeschreibung**
	Der *Verantwortliche*, ein *Auftragsverarbeiter* oder eine eigenmächtig handelnde, zugriffsberechtigte Person verarbeitet personenbezogene Daten in zweck- bzw rechtswidriger Weise weiter.
	Risikoquelle
	Interne / Externe menschliche Risikoquellen: • Interne Mitarbeiter*innen • Staatliche Institutionen (Nachrichtendienste, Strafverfolgung) **Interne technische Risikoquellen:** • Softwarearchitektur
	Risikoursache
	• Unbefugte oder unrechtmäßige Verarbeitung • Unbefugte Offenlegung von und Zugang zu Daten zB durch einen *Verantwortlichen* an anderen beteiligten *Verantwortlichen*, dem Zugang nicht zustünde • Verwendung der Daten durch die Verantwortlichen zu inkompatiblen Zwecken/Verarbeitung wider den Zweckbindungsgrundsatz (etwa zur Ausforschung von Personen)
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Zugriff auf und Verarbeitung von personenbezogenen Daten zum wirtschaftlichen oder beruflichen Nachteil der Betroffenen • Diskriminierung durch gezieltes Auslesen spezifischer personenbezogener Daten und deren schädliche Verwendung gegen die Betroffenen **Immaterielle Schäden:** • 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 da eine große Anzahl an Datensätzen betroffen sein kann.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	• Zuweisung von Rollen durch gesetzliche Bestimmungen bzw *Auftragsverarbeitervereinbarungen* • 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)

5.2.12 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 *Verantwortliche* 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: • Entscheidungsträger*innen des *Verantwortlichen* • Interne Mitarbeiter*innen **Interne technische Risikoquelle:** • Systemkomplexität
	Risikoursache
	• Unzureichende Informationserteilung • Unzureichende Informationsaufnahme durch die betroffene Person
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden • 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**
	• Es wird eine Datenschutzerklärung in einfacher und klarer Sprache bereitgestellt.[212] • Das System wird über die Website oesterreich.gv.at via FAQs zu Sicherheit und Datenschutz grundlegend erklärt.[213]

[212] Die Datenschutzerklärung kann in der entsprechenden Applikation sowie auf der Website des Verantwortlichen abgerufen werden.
[213] https://www.oesterreich.gv.at/id-austria/haeufige-fragen.html; https://www.oesterreich.gv.at/eausweise/haeufige-fragen/haeufige-fragen-eausweise-sicherheit.html (abgerufen am 23.08.2023).

	• 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)

5.2.13 Nutzung der Ökosysteme von Google und Apple

1) Risikoidentifikation	**Risikobeschreibung**
	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.[214] Dem kann entgegengehalten werden, dass sich die betroffenen Personen bereits auf dieser Infrastruktur befänden 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.
	Risikoquelle
	Interne / Externe menschliche und strukturelle Quelle: • Entscheidungsträger*innen des *Verantwortlichen* • Externe Entscheidungsträger*innen
	Risikoursache
	• Management-Entscheidung auf Seiten des *Verantwortlichen* zur Nutzung der Infrastruktur von Google und Apple als Plattformprovider für die Distribution der eAusweise-App. Man sieht sich aus Sicht des *Verantwortlichen* dazu gezwungen, auf die Plattformen und Technologien Dritter zurückzugreifen, um digitale Ausweise und Nachweise 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

	börsennotierten US-amerikanischen IT-Konzernen, da keine eigene Distributionsplattform ohne Weiterverarbeitung der Nutzer*innendaten zu Werbezwecken verwendet wird • Datenverarbeitung wird nicht auf das notwendige Maß beschränkt; insuffiziente Umsetzung des Grundsatzes der Datenminimierung • Verarbeitung von personenbezogenen Daten zu inkompatiblen Zwecken (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
	Immaterielle Schäden: • Gesellschaftliche und soziale Nachteile (durch weitere Monopolisierung privater IT-Konzerne); strukturelle Schädigung der Privatsphäre (Tracking über Webseiten, Applikationen und Endgeräte hinweg); „chilling effects“, wenn Menschen davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit zu entfalten

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Maximal (4) Kommentar: Das Risiko ist bereits eingetreten.	Wesentlich (3)	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Physische Ausweise und Nachweise 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.[215]

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.[216]

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

[215] Siehe Art 5 Abs 2 sowie Art 35 Abs 11 DSGVO.
[216] 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 Zugriffsrechten unterliegen;
- die Protokollierung auf das technisch notwendige Minimum beschränkt ist und insbesondere Vorgänge des Vorweisens und Überprüfens von Ausweisen im System der Ausweisplattform nicht protokolliert werden;

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.[217]

[217] 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)[218]
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
BGBl:	Österreichisches Bundesgesetzblatt; “I” steht in diesem Zusammenhang für den ersten Teil, in dem Gesetze kundgemacht werden, in Teil “II” wiederum Verordnungen und in Teil “III” Staatsverträge.
Bitkom:	Deutscher Bundesverband der Informationswirtschaft und Telekommunikationsbranche
BlgNR:	Beilagen zu den stenographischen Protokollen des Nationalrates[219]
BMDW:	Bundesminister für Digitalisierung und Wirtschaftsstandort
BMF	Bundesministerium für Finanzen
BMG:	Bundesministeriengesetz 1986 BGBl I 1986/76

[218] Siehe *Dax/Hopf*, Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europäische Rechtsquellen[8] (2019) 43.
[219] *Dax/Hopf*, AZR[8] 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[220] 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 *Verantwortlichen* 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

[220] Vgl *Feik/Randl* in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[3] (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, ABl 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, ABl L 1995/281, 31
E-GovG:	E-Government-Gesetz; Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, BGBl I 2004/10
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 Rechtlinie 1999/93/EG, ABl 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:	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 Personenkennzeichen 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.[221]
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)

[221] 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[222]
StVO:	Straßenverkehrsordnung 1960 BGBl I 1960/159
SZRB:	Stammzahlenregisterbehörde; nunmehr im Wirkungsbereich des BMF[223]
tlw:	teilweise
TOM(s):	(geeignete) technische und organisatorische Maßnahmen gem DSGVO[224]
ua:	unter anderem
UDID:	Unique Device Identifier; eindeutige Gerätenummer für Apple-Produkte
uE:	unseres Erachtens
usw:	und so weiter
uU:	unter Umständen
vbPK-VT:	verschlüsseltes bereichsspezifisches Personenkennzeichen des Bereichs Verkehr und Technik
VDA:	*Vertrauensdiensteanbieter*; ein Dienst, der elektronische Signaturen, Siegel oder Zertifikate erstellt, überprüft und validiert sowie aufbewahrt[225]
vgl:	vergleiche
VO:	Verordnung

[222] Vgl § 2 Z 8 E-GOVG.
[223] Siehe erläuternd https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 23. 8.2023).
[224] Siehe etwa Art 24, 32 DSGVO.
[225] https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/anbieter/liste_der_vertrauensdiensteanbieter/Anbieter.de.html.

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