Digitaler Nachweis der Identität
Datenschutz-Folgenabschätzung

Research Institute – Digital Human Rights Center

DSFA-Bericht Digitaler Nachweis der Identität | 2024

https://researchinstitute.at

Digitaler Nachweis der Identität

Datenschutz-Folgenabschätzung

Bericht zur Datenschutz-Folgenabschätzung des digitalen Nachweises der Identität im Auftrag des Bundeskanzleramts (BKA)

Wien, Mai 2024

Autoren:
Christof Tschohl
Jan Hospes
Philipp Poindl
Walter Hötzendorfer
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	22.12.2023	V 0.1	Erstellung der internen Berichtsstruktur	Jan Hospes	Berichtsstruktur
2	09.01.2024	V 0.3	Erste Version des Sachverhalts, der Rechtsgrundlagen und der Rollen festgehalten	Jan Hospes	in Arbeit
3	25.01.2024	V 0.4	Ausführungen zu Risikobeurteilung	Jan Hospes	in Arbeit
4	26.01.2024	V 0.5	Ausführungen zu Betroffenenrechten, Verarbeitungsgrundsätzen,	Jan Hospes	in Arbeit
5	28.01.2024	V 0.6	Vorbereitung für internes Review	Jan Hospes	in Arbeit
6	29.04.2024	V 0.7	Vorbereitung für gesamtheitliche Entwurfsfassung	Jan Hospes	präfinal für Review durch Auftraggeber
7	08.05.2024	V 0.8	Einarbeitung von Feedback von Auftraggeber	Jan Hospes	präfinal für internes Review
8	15.05.2024	V 0.9	Einarbeitung von internem Feedback	Jan Hospes	präfinal für Besprechung von Detailfragen mit Auftraggeber
9	21.05.2024	V 0.99	Einarbeitung von letztem Feedback	Jan Hospes	präfinal
10	17.06.2024	V 1	Einarbeitung Feedback Stakeholder	Christof Tschohl	final

Disclaimer

Sofern im Folgenden nicht anders angegeben, wurden alle Internetlinks zuletzt am 15.05.2024 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 den digitalen Nachweis der Identität (folgend auch digitaler Identitätsnachweis). Der digitale Nachweis der Identität ist eine Funktion der Ausweisplattform, welche es Nutzer*innen ermöglicht, mittels der eAusweise App die eigene Identität gegenüber Privaten oder der Exekutive, welche sich physisch in direkter Nähe einer Nutzer*in befinden, digital nachzuweisen. Nutzer*innen wird es somit künftig deutlich leichter fallen, einen Nachweis der Identität an der Person mitzuführen, ohne den klassischen Risiken wie Verlust und Diebstahl eines physischen Dokuments ausgesetzt zu sein. Die Möglichkeit, physische Ausweise und Nachweise zu verwenden, bleibt wie bisher unverändert und uneingeschränkt bestehen.

Der digitale Nachweis der Identität baut auf der ID Austria und auf der Ausweisplattform auf. Zu beiden Systemen wurde jeweils gesondert eine DSFA durchgeführt sowie der zugehörige DSFA-Bericht veröffentlicht.[1] [2]

Wenn der digitale Nachweis der Identität (so wie andere Ausweise/Nachweise auch) in der eAusweise-App geführt wird, können Identitätsdaten gegenüber Exekutivorganen oder Privaten vorgewiesen werden.

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

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

- Nachweis der Identität laden und anzeigen;
- Identität gegenüber Exekutivorganen nachweisen;
- Nachweis der Identität gegenüber Privaten vorweisen;
- Nachweis der Identität aktualisieren;

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

Den Kern der DSFA bildet die datenschutzrechtliche Risikoanalyse, die eine Reihe von Risiken für die Rechte und Freiheiten der betroffenen Personen aufzeigt sowie diese Risiken und die diesbezüglich getroffenen Maßnahmen in methodisch-systematischer Weise in ihrer Eintrittswahrscheinlichkeit und Schwere analysiert und bewertet. Dabei werden neben solchen Risiken, die mit nahezu jeder Verarbeitung personenbezogener Daten unweigerlich verbunden sind, insbesondere auch das Potenzial zur

[1] https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 15.05.2024).

[2] https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

Überwachung und die dagegen getroffenen Maßnahmen behandelt sowie Fragen der Freiwilligkeit der Nutzung des Systems und das Thema einer möglichen Überforderung der betroffenen Personen, die Datenverarbeitung und ihre Konsequenzen zu verstehen.

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

Die vorliegende DSFA kommt zu dem Ergebnis, dass die identifizierten verbleibenden Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der gesetzten Maßnahmen des Verantwortlichen nicht als hoch einzustufen sind und somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Art 36 DSGVO besteht. Die Notwendigkeit und Verhältnismäßigkeit der untersuchten Datenverarbeitungsprozesse werden auf Basis der entsprechenden systematischen Analyse in Verbindung mit den Rechtsgrundlagen und unter Berücksichtigung aller technischen und organisatorischen Maßnahmen als gegeben erachtet.

Zusammenfassend kann somit festgehalten werden, dass

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

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

Künftig gilt es die weitere technische, rechtliche und gesellschaftliche Entwicklung sorgfältig zu beobachten und die Auswirkung auf die Rechte und Freiheiten natürlicher Personen laufend zu prüfen. Dabei ist neben möglicher unbefugter Verarbeitung personenbezogener Daten insbesondere auf Diskriminierung und Ungleichbehandlung zu achten. In diesem Sinne betrachtet die DSFA nicht nur die Risiken für die Rechte und Freiheiten einzelner Individuen, sondern wahrt auch den Blick auf die gesamte Gesellschaft.

Den *Verantwortlichen* trifft eine aktive Monitoring-Verpflichtung im Hinblick auf alle für das System relevanten tatsächlichen oder rechtlichen Umstände. Lassen sich wesentliche Änderungen in der Risikolage identifizieren, sind jedenfalls angemessene technische und organisatorische Anpassungen der Maßnahmen für eine datenschutzkonforme Verarbeitung der personenbezogenen Daten vorzunehmen.

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

2 Einleitung

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

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

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

An dieser Stelle bedarf es zum besseren Verständnis der im Folgenden verwendeten unterschiedlichen Ressortbezeichnungen des Auftraggebers des Hinweises, dass es während der Arbeiten an diesem Bericht zu einem Übergang der Zuständigkeit für die *Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung für das Service und die Interaktion mit Bürgern und Unternehmen* und damit der zuständigen Abteilung *e-Government Bürger* als Teil der Sektion *Digitalisierung und e-Government* vom BMF hin zum im *Bundeskanzleramt* (BKA) eingerichteten Staatssekretariat unter der Leitung von Frau Staatssekretärin Claudia Plakolm kam. Soweit als möglich gelangt die in diesem Zusammenhang jeweils historisch korrekte Ressortbezeichnung zum Einsatz.

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.

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

[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.

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 Darstellung des Sachverhalts und Spezifizierung des Prüfgegenstands

Der digitale Nachweis der Identität bietet Nutzer*innen die Möglichkeit, die eigene Identität einem Gegenüber digital anzuzeigen. Umgekehrt können Exekutivorgane oder andere Dritte (zB Privatpersonen im Zuge eines Vertragsabschlusses) die Identität prüfen. Der digitale Nachweis der Identität baut wesentlich auf der Architektur der Ausweisplattform des BKA auf und wird als spezifischer Verarbeitungszweck bzw. als eigenständige Funktion der Ausweisplattform beleuchtet.

Der digitale Nachweis der Identität ist keine exakte digitale Abbildung eines bestehenden, analogen Ausweises, sondern ein eigener, neuer Nachweis. Die österreichische Rechtsordnung kennt keine einheitliche Definition eines amtlichen Lichtbildausweises, es ist sohin nicht allgemeingültig definiert, wodurch (durch welche Attribute) die Identität einer Person bestimmt ist.

Im Rahmen der Schaffung des digitalen Nachweises der Identität wurde eine Festlegung getroffen, welche Attribute zweckdienlich sind, um eine Prüfung der Identität einer Person zu ermöglichen. Nach dem Grundsatz der Datenminimierung sollen Personen nur die notwendigen Daten für einen eindeutigen Nachweis der Identität bereitstellen. Die Berücksichtigung dieses Grundsatzes spiegelt sich etwa in der Exklusion der Wohnadresse beim Nachweis der Identität wider.

[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).

Identitätsdaten werden über die ID Austria geladen und als Attribute an die eAusweise-App übergeben. Die Daten dürfen dann offline gespeichert und verwendet werden, wobei der Zeitpunkt der letzten Aktualisierung angezeigt wird.

3.1 Systemarchitektur

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

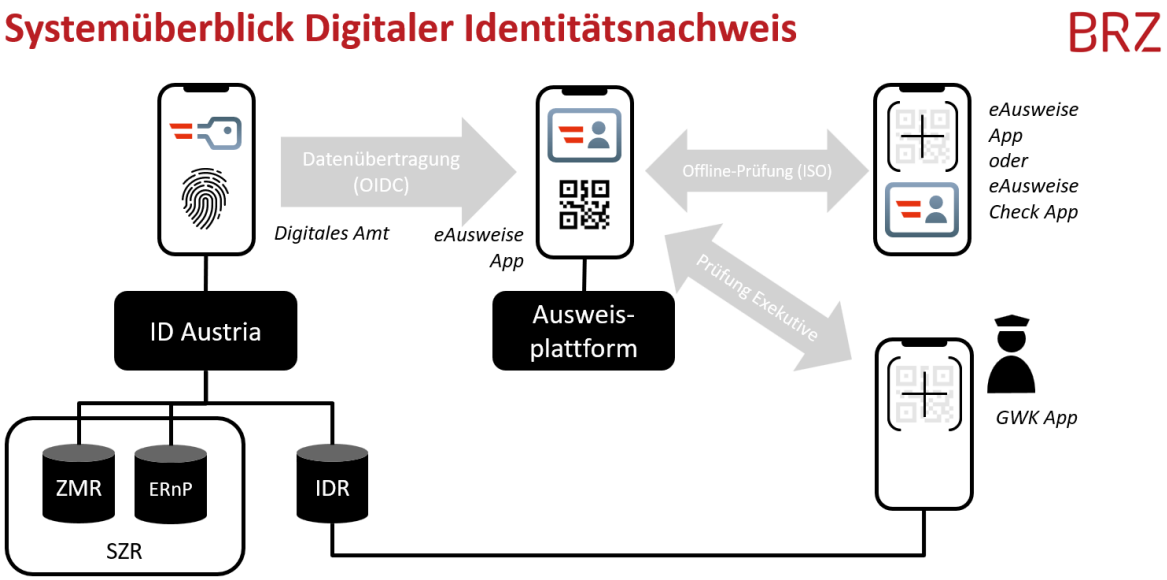

Abbildung 1: Überblick über die Funktionsweise des digitalen Nachweises der Identität basierend auf der eAusweise-App/Ausweisplattform und ID-Austria

Ausweisplattform (AWP)

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

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.

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

[11] https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 15.05.2024).

[12] https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

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

GWK Check-App

Die Gemeindewachkörper bekommen zur Erfüllung der ihnen übertragenen Aufgaben die GWK Check-App zur Verfügung gestellt. Diese App kann über ein eigenes Backend im Bundesrechenzentrum Daten laden und anzeigen.

IDR

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

ZMR / ERnP

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

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

Minimum Data Set

[13] https://www.oesterreich.gv.at/lexicon/Z/Seite.991731.html (abgerufen am 15.05.2024).
[14] https://www.oesterreich.gv.at/lexicon/E/Seite.991096.html (abgerufen am 15.05.2024).

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

Open ID Connect OIDC

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

ISO

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

3.2 Prüfgegenstand

Gegenstand der vorliegenden DSFA sind daher die nachfolgend angeführten Verarbeitungstätigkeiten:

- **Nachweis der Identität laden und anzeigen;** [15]
- **Identität gegenüber Exekutivorganen nachweisen;** [16]
- **Nachweis der Identität gegenüber Privaten vorweisen;** [17]
- **Nachweis der Identität aktualisieren;** [18]

Die angebundenen Register (ZMR/ERnP/IDR) stellen keinen Gegenstand der vorliegenden DSFA dar, da diese unabhängig von Ausweisplattform und digitalem Nachweis der Identität der Verantwortlichkeit des jeweils zuständigen Bundesministeriums unterliegen.

Gänzlich außerhalb der Verantwortlichkeit des BKA und daher nicht Gegenstand der vorliegenden DSFA ist die Verarbeitung personenbezogener Daten durch Organe der Bundespolizei im Zuge einer Überprüfung des digitalen Identitätsnachweises einer Person, dies fällt in die datenschutzrechtliche Verantwortlichkeit des Bundesministeriums für Inneres (BMI) bzw der Landespolizeidirektionen (LPD). Sehr wohl Gegenstand der vorliegenden DSFA ist die - durch das BKA betriebene - GWK Check-App, mit Ausnahme der Verarbeitung der personenbezogenen Daten der Organe der Gemeindewachkörper in ihrer Rolle als Nutzer*innen der GWK Check-App.

Zur Abgrenzung der verschiedenen datenschutzrechtlichen Verantwortlichkeiten im Detail siehe Abschnitt 4.3.

3.3 Die einzelnen Datenverarbeitungstätigkeiten

Im Folgenden wird eine funktionale Perspektive und vor allem die Perspektive der datenschutzrechtlich betroffenen Personen eingenommen, um den Gegenstand der vorliegenden DSFA und seine Komponenten, die oben bereits beschrieben wurden, in einzelne Verarbeitungstätigkeiten zu gliedern. Dies dient der Strukturierung des Untersuchungsgegenstandes aus datenschutzrechtlicher Sicht. Jedes der

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

nachfolgenden Kapitel beschreibt eine Verarbeitungstätigkeit. Die darauffolgende datenschutzrechtliche Analyse folgt dieser Struktur.

3.3.1 Nachweis der Identität laden und anzeigen

Zweck dieser Verarbeitungstätigkeit ist es, für den digitalen Identitätsnachweis notwendige Daten auf das Endgerät der Nutzer*in zu laden. Das ist erforderlich, um den digitalen Identitätsnachweis vorzeigen zu können und ist somit Voraussetzung für die nachfolgend beschriebenen Verarbeitungstätigkeiten. Dazu wählt die Nutzer*in in der eAusweise-App nach biometrischer Authentifizierung die entsprechende Funktion zum Herunterladen des digitalen Nachweises der Identität auf das eigene Endgerät aus. Daraufhin springt die Benutzer*in in die „Digitales Amt App", führt eine Anmeldung an der ID-Austria durch und bezieht ein Registrierungstoken (ID-Token) mittels dessen die Ausweisplattform die Identitätsdaten[19] vom ID-Austria-System lädt.

Die Ausweisplattform bereitet Identitätsdaten als ISO-kompatible-Struktur auf und übermittelt diese signiert an die eAusweise-App.[20] Der geladene Nachweis der Identität ist maximal 3 Monate oder bis zum Ablauf des Gerätezertifikats gültig.

Die wesentliche Information über erfolgte Verarbeitungsvorgänge, nämlich ob eine bestimmte betroffene Person ihren digitalen Identitätsnachweis auf ihr Endgerät geladen oder sich an der ID-Austria angemeldet hat, kann sich aus einem Protokolleintrag im jeweiligen System ergeben.[21] Zu beachten ist zudem in diesem Zusammenhang, dass gemäß § 16a Abs 12 iVm § 14 Abs 5 MeldeG[22] aufseiten des zentralen Melderegisters bzw nach § 22b Abs 5 PassG[23] für das Identitätsdokumentenregister – und somit außerhalb der Systemgrenzen der Ausweisplattform und der hierin darzustellenden Zuständigkeit des BKA – eine Protokollierung aller tatsächlich durchgeführten Verarbeitungsvorgänge und somit auch von Datenabfragen im Zuge des Ladens und von Aktualisierungen der Identitätsdaten durchgeführt wird, aus der erkennbar ist, welcher Person welche Daten aus diesem Register übermittelt wurden, wobei die Protokolldaten für drei Jahre aufzubewahren sind.

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

Identitätsdaten und das Datum der letzten Aktualisierung können in der eAusweise-App gesichtet oder zur Prüfung vorgelegt werden.

---

[19] Siehe Abschnittsende.

[20] Die Signaturlaufzeit wird dabei an die Zertifikatslaufzeit der jeweiligen ID Austria angepasst.

[21] Siehe zur Protokollierung der ID Austria 4.6 der DSFA zur ID-Austria sowie die DSFA zur Ausweisplattform https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

[22] Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 – MeldeG) BGBl I 1992/9.

[23] Bundesgesetz betreffend das Passwesen für österreichische Staatsbürger (Passgesetz 1992) BGBL I 1992/839 idF 2021/123.

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

Folgende Daten werden hierbei verarbeitet:

- Vorname (Datenquelle: ZMR oder ERnP)
- Familienname (Datenquelle: ZMR oder ERnP)
- Geburtsdatum (Datenquelle: ZMR oder ERnP)
- Lichtbild (Datenquelle: IDR)
- bPK[24]
- IP-Adresse des Mobilgeräts
- Status der ID Austria (Voll- oder Basisfunktion)
- Registrierungstoken (ID-Token)

3.3.2 Identität gegenüber Exekutivorganen nachweisen

Zweck dieser Verarbeitungstätigkeit ist das Vorweisen und Überprüfen der Identitätsdaten im Zuge einer Überprüfung des digitalen Nachweises der Identität einer Person, wenn die Nutzer*in dies gegenüber dem Vorweisen eines physischen Ausweises bevorzugt.

Im Fall der Überprüfung des digitalen Nachweises der Identität einer Person erfolgt diese, anders als in allen anderen Fällen der Verwendung des digitalen Identitätsnachweises, durch Abruf dieser Daten aus den Registern (ZMR/ERnP/IDR) durch das befugte Organ, das die Überprüfung durchführt. Für diesen Zweck wird durch Vorweisen des mittels eAusweise-App erstellten QR-Code durch die Nutzer*in dem Endgerät des Organs mitgeteilt, von welcher Person Daten aus den Registern abgerufen (vgl. §22b PassG) werden müssen.

3.3.2.1 Vorweisen durch die Nutzer*in

Die Nutzer*in öffnet die eAusweise-App, führt eine biometrische Authentisierung durch und trifft im Anwendungsfall “Vorzeigen” der eAusweise-App die Auswahl, ihre Identität gegenüber der Exekutive nachzuweisen. Es wird daraufhin ein QR-Code erstellt und angezeigt, welcher daraufhin dem Organ (der Bundespolizei oder der Gemeindewachkörper) vorgewiesen werden kann, um diesem den Abruf der Identitätsdaten der Nutzer*in aus (ZMR/ERnP/IDR) zu ermöglichen, wie in der folgenden Abbildung schematisch dargestellt:

[24] 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 BKA 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).

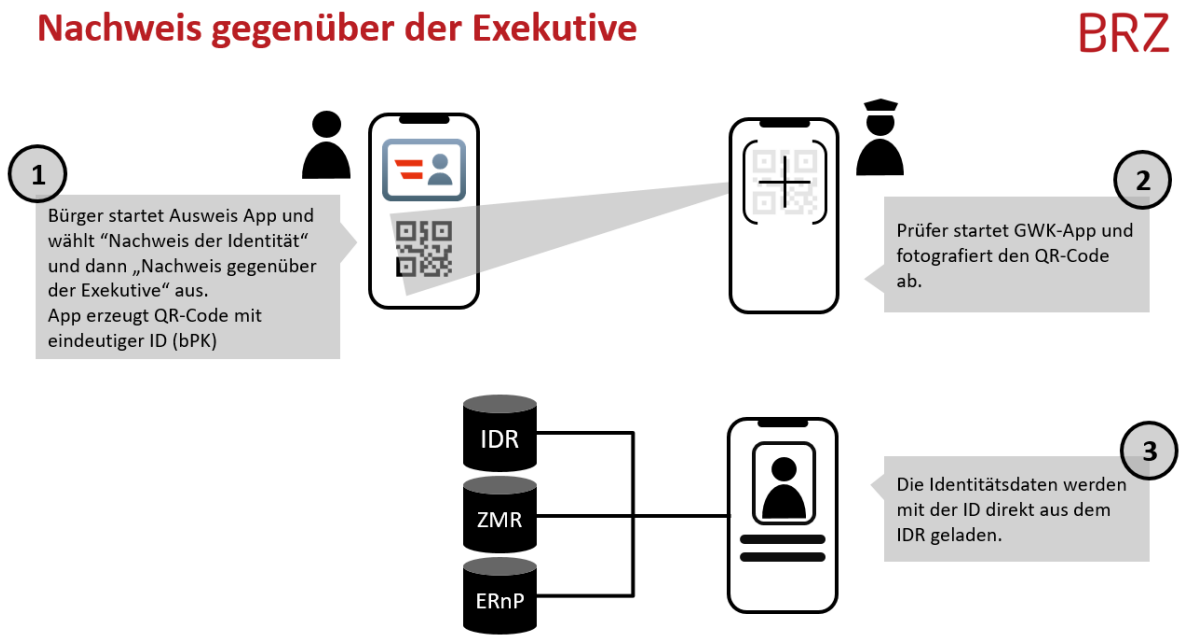

Abbildung 2: Schematischer Ablauf eines Nachweises gegenüber der Exekutive

Im Falle der Gemeindewachkörper erfolgt dies mittels der GWK Check-App auf dem dienstlichen Endgerät des Organs. Das Organ fotografiert mit der GWK Check-App den QR-Code ab. Die GWK Check-App prüft daraufhin unter Einbeziehung der Widerrufsliste[25] die Signatur. Über das im QR-Code enthaltene bPK wird dem Organ ermöglicht, die Identitätsdaten der betroffenen Person aus den Registern auf sein Endgerät zu laden.

Dieser QR-Code enthält auch einen (signierten) Timestamp, wodurch eine Wiederverwendung des QR-Codes verhindert werden soll.[26]

Darüber hinaus enthält der QR-Code auch die Attribute Vorname, Nachname, Geburtsdatum, die gemeinsam den MDS bilden. Zudem sind die im QR-Code enthaltenen Daten, wie erwähnt, mit einer Signatur versehen.

Folgende Daten werden somit in diesem Schritt wie beschrieben verarbeitet:

- vbPK
- MDS
- Timestamp
- Signatur dieser Daten

Die genannten Daten sind hierbei in dem QR-Code unverschlüsselt enthalten.

[25] Siehe DSFA Ausweisplattform: https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

[26] Denn gem § 4 Abs 6 E-GovG ist dies nur *Inhabern* eines E-ID, die die eAusweise-App verwenden möglich. Die Zeitspanne bis zur Kontrolle darf dabei bis zu 15 Minuten betragen.

Folgende Algorithmen kommen zum Einsatz:

ECC-Basiert:

- JWT Algorithmus: ES256
- verwendete Kurve: secp256r1 (Standard NIST Kurve)
- Algorithmus:
    - Signatur: ECDSA
    - Hash: SHA256
- Schlüssellänge: 256 bit

Fallback bei älteren Geräten (sollte keine EC Crypto unterstützt werden): RSA-Basiert:

- JWT Algorithmus-Suite: PS256
- verwendete Algorithmen
    - Signatur: RSASSA-PSS
    - Hash: SHA256
- Schlüssellängen: 3072 bit

3.3.2.2 Einsichtnahme in die Register (ZMR/ERnP/IDR) durch das jeweilige Organ mittels GWK Check-App

Die Nutzer*innenauthentifizierung für die Organe der Gemeindewachkörper in der GWK Check-App, die für die Einsichtnahme in die Register stets erforderlich ist, erfolgt durch eine Anmeldung mittels ID-Austria, und zwar mit der persönlichen Identität des jeweiligen Organs. Es handelt sich daher um denselben Anmeldevorgang, welcher in der DSFA zur Ausweisplattform[27] beschrieben wurde, insb muss sich die Digitales-Amt-App ebenfalls auf demselben Gerät wie die GWK Check-App befinden. Bei der Anmeldung über die ID Austria wird das bPK des jeweiligen Organs mittels eines Web-Tokens im OIDC-Standard übergeben und es wird damit die Authentisierung am GWK Check-Backend durchgeführt. Das GWK Check-Backend versucht daraufhin, über das bPK die Daten des jeweiligen Organs zu laden. Sofern dies erfolgreich ist, bleibt das Organ maximal für die Dauer der Session von 14 Stunden angemeldet, ansonsten erfolgt ein Abbruch.

Werden entsprechende dienstliche Geräte gemeinsam verwendet, muss die Anmeldung für das jeweilige Organ immer wieder neu durchgeführt werden.

[27] Siehe DSFA Ausweisplattform: https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

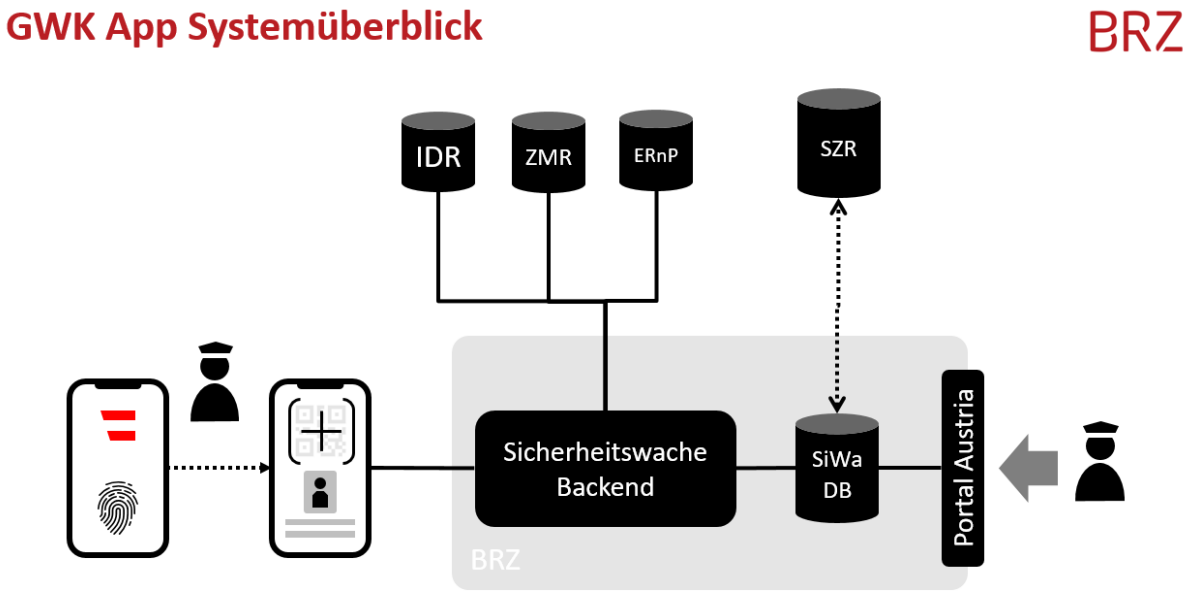

Abbildung 3: Überblick über GWK Check-App und GWK-Backend

Die Administration der jeweiligen Organe für die Zwecke dieser Applikation erfolgt in einer eigenen Admin-App über das Portal Austria. Diese Administration wird von den Gemeindewachkörpern selbst durchgeführt. Dabei werden die jeweiligen Organe über eine Personensuche im Stammzahlenregister mit dem jeweiligen bPK in der entsprechenden GWK Check-Datenbank angelegt.

Hat sich das jeweils tätige Organ in der GWK Check-App erfolgreich authentifiziert, kann diese zum Auslesen eines QR-Codes im Zuge einer des Nachweises verwendet werden. Wie oben ausgeführt, ermöglichen die im QR-Code enthaltenen Daten der jeweiligen Nutzer*in der eAusweise-App dem tätigen Organ, die Identitätsdaten dieser Nutzer*in aus den Registern auf das dienstliche Endgerät zu laden.[28] Darüber hinaus sind, wie erwähnt, ein Timestamp und die App-Signatur im QR-Code enthalten, womit auf dem dienstlichen Endgerät zunächst über die Prüfung dieser Signatur bzw der damit signierten Daten unter Einbeziehung der Widerrufsliste[29] überprüft wird, ob der QR-Code aktuell ist.[30] Dies ist erforderlich, weil gemäß § 4 E-GovG die eindeutige Identifikation einer natürlichen Person durch Personenbindung die rechtmäßige Inhaberschaft der ID Austria voraussetzt. Das Vorzeigen eines Screenshots oder gar eines Ausdrucks des QR-Codes, was ansonsten im gegenständlichen Anwendungsfall technisch möglich wäre, wird auf diese Weise ausgeschlossen, um den genannten gesetzlichen Anforderungen zu genügen.

[28] Im Rahmen dieses Anwendungsfalles ist daher weder eine Aktualisierung des vbPK erforderlich (denn dieses ändert sich nicht) noch eine Aktualisierung der Daten auf dem Mobilgerät der Nutzer*innen, denn das jeweilige Organ nimmt dabei selbst Einsicht in die Register.

[29] Siehe DSFA Ausweisplattform: https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

[30] Wie oben bereits erwähnt, darf die Zeitspanne bis zu 15 Minuten betragen.

Ist diese Prüfung erfolgreich, werden die Daten aus den Registern geladen. Die Zugriffe führt das GWK Check-Backend durch und gibt die Daten an die App zurück.

Neben der in diesem Kapitel bereits beschriebenen Funktion des QR-Code-Scans und anschließender Abfrage bzw Anzeige verfügt die GWK Check-App über keine weiteren Abfragemöglichkeiten. Die hierbei verarbeiteten Datenkategorien wurden nach den Maßgaben des § 4 E-GovG unter Beachtung der Grundsätze der Datenminimierung gewählt.

3.3.3 Nachweis der Identität gegenüber Privaten vorweisen

Zweck dieser Verarbeitungstätigkeit ist das Vorweisen und Überprüfen des digitalen Nachweises der Identität in allen anderen Fällen außer des Nachweises der Identität gegenüber Exekutivorganen gegenüber einer Nutzer*in der eAusweise-App oder eAusweis-Check-App.

Die Prüfer*in wählt in der eAusweise-App oder eAusweis-Check-App die Überprüfungsfunktion aus und wählt in der eAusweise-App die Funktion zur Prüfung des digitalen Nachweises der Identität aus.

Parallel öffnet die nachweisende Nutzer*in die eAusweise-App, führt eine biometrische Authentisierung durch und trifft im Anwendungsfall “Vorzeigen” der eAusweis-App die Auswahl, ihre Identität gegenüber Dritten (also nicht der Exekutive wie in 3.3.2 beschrieben) nachzuweisen.

Daraufhin wird das letzte Aktualisierungsdatum und die Information, dass ein QR-Code generiert wird, um eine Datenverbindung mit einem prüfenden Gerät aufzubauen, angezeigt. Die Nutzer*in bestätigt mit „QR-Code erstellen“, woraufhin ein QR-Code mit einem Einmal-Token bzw Device Engagement Code (DEC) angezeigt wird. Dieser kann daraufhin zur Überprüfung vorgezeigt werden. Übermittlung und Überprüfung folgen dabei dem internationalen Standard ISO/IEC 18013-5. Der Datenaustausch besteht hierbei aus drei Phasen: Initialisierung, Device Engagement und Data Retrieval.[31]

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

Nachdem dieser QR-Code durch die Prüfer*in gescannt wurde, beginnt die Phase Data Retrieval. Dazu bauen die involvierten Mobilgeräte eine verschlüsselte Verbindung über Bluetooth low energy auf und es werden die Daten vom Endgerät der sich ausweisenden Person auf jenes der überprüfenden Person übertragen. Zur Verschlüsselung dieser Verbindung kommt der Standard AES-256-GCM zum Einsatz

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

und das entsprechende Schlüsselpaar wird jeweils über HKDF gemäß RFC 5869 erzeugt.[32] Der Vorgang kann vor jedem Schritt abgebrochen werden.

Anschließend werden die Daten verifiziert (die Signatur mit dem entsprechenden App-Zertifikat überprüft) und auf dem Gerät der überprüfenden Person angezeigt. Der gesamte Überprüfungsvorgang erfolgt offline, die mobilen Geräte benötigen hierzu grundsätzlich[33] keine Internetverbindung und dieser Vorgang wird somit auch serverseitig nicht erfasst.

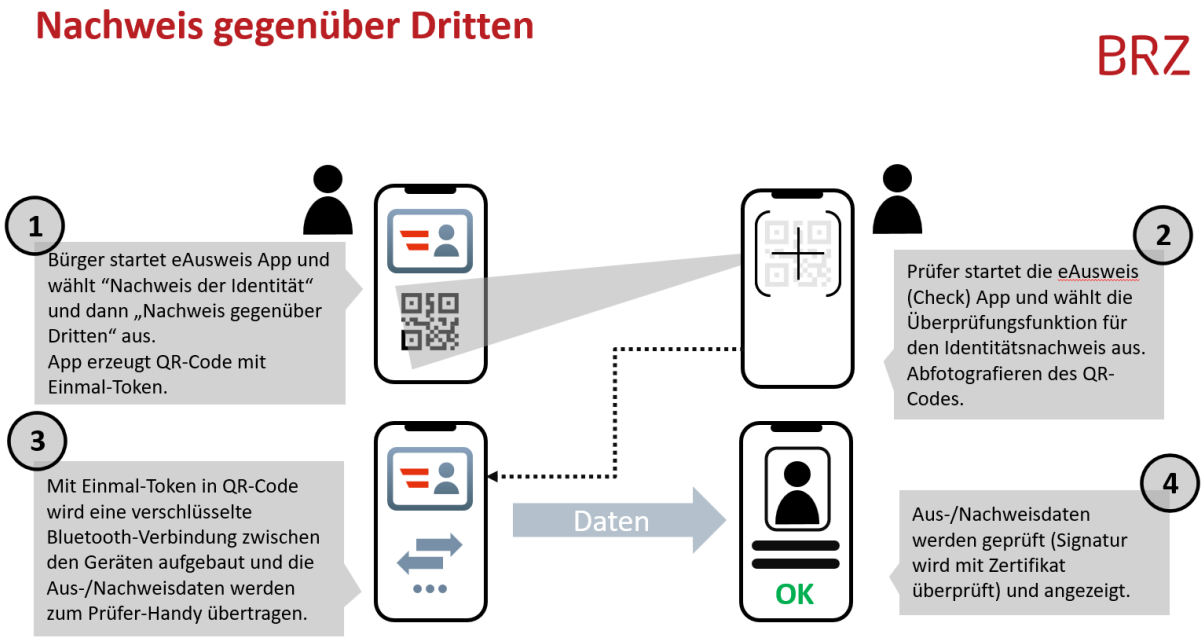

Abbildung 3: Ablauf des Nachweisvorgangs offline

Folgende Daten der Nutzer*in werden hierbei verarbeitet:

- Vorname
- Familienname
- Geburtsdatum
- Lichtbild
- bPK[34]

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

[33] Mit Ausnahme einer allfälligen Aktualisierung der Widerrufsliste auf dem Endgerät der überprüfenden Person beim Öffnen der App, wenn eine Internetverbindung besteht, und der Aktualisierung der Ausweisdaten auf dem Endgerät der sich ausweisenden Person innerhalb der vorangegangenen 30 Minuten, wenn ein Nachweis der Identität erfolgen soll.

[34] 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 BKA 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).

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

3.3.4 Nachweis der Identität aktualisieren

Zweck dieser Verarbeitungstätigkeit ist es, die Identitätsdaten zu aktualisieren. Der Nutzer*in werden nach Auswahl der Funktion Informationen eingeblendet und er*sie wird in die App „Digitales Amt“ geleitet. Dort erfolgt eine Anmeldung an der ID-Austria und Daten werden entsprechend der Funktion „Nachweis der Identität laden und anzeigen“ (siehe 3.3.1) neu geladen.

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 ergeben.

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.[35]

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);

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

– Garantien in Bezug auf die internationale Übermittlung von Daten.[36]

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.[37] 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.[38] 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.[39]

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[40], IMSI[41], UDID[42], MSISDN[43]), die Identität des Telefons[44], Kreditkarten- und Zahlungsdaten oder auch der Browserverlauf als personenbezogene Daten zu werten sind.[45] Weitere gängige Angaben mit identifizierendem Bezug zu einer natürlichen Person sind zB Handynummer[46], E-Mail-Adresse, Sozialversicherungsnummer[47], KFZ-Kennzeichen[48], IP-Adresse[49] und auch medizinische Diagnosen.[50]

---

[36] 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.

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

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

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

[40] *International Mobile Equipment Identity* – eindeutige Nummer des Endgeräts.

[41] *International Mobile Subscriber Identity* – eindeutige Nummer des Netzteilnehmers.

[42] *Unique Device Identifier*– eindeutige Gerätenummer für Apple-Produkte.

[43] *Mobile Station Integrated Services Digital Network* – weltweit eindeutige Mobilfunk-Rufnummer.

[44] 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".

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

[46] *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013, 10.

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

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

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

[50] *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9 DSGVO.

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.[51] Die Information kann sich zusammensetzen aus sachbezogenen Aussagen zu Verhältnissen oder überprüfbaren Eigenschaften sowie Einschätzungen und Urteilen über die betroffene Person. Der Personenbezug von Daten kann wiederum durch jene Information hergestellt werden, welche ein Inhaltselement, Zweckelement oder Ergebniselement beinhaltet. Der dritte wesentliche Faktor bei der Qualifikation von personenbezogenen Daten gem Art 4 Z 1 DSGVO richtet sich auf die betroffene Person, bei der es sich immer um eine natürliche Person handeln muss. Der 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.[52] 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.[53] 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*

[51] Vgl *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 8.
[52] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[53] *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.

die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."

Die Literatur[54] und unionsrechtliche Judikatur[55] setzen am sogenannten „*relativen Personenbezug"* bzw der "*relativen Theorie*"[56] an, wonach für die Bestimmung der Identifizierbarkeit die Kenntnisse und Mittel der datenverarbeitenden Stelle und nicht irgendeines *Dritten* ausschlaggebend sind. Sofern der *Verantwortliche* Einzelangaben einer Person durch relevantes Zusatzwissen[57] [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.[58] 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.*"[59]

4.1.2 Personenbezogene Daten im System

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

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.[60] 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,[61] und daher zum Schutz personenbezogener Daten wesentlich beiträgt. Dementsprechend sind im gegebenen Fall jedenfalls auch

[54] 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.

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

[56] 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.

[57] 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).

[58] Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.

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

[60] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.

[61] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.

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.

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.[62] Für die vorliegende Verarbeitung von personenbezogenen Daten gem Art 4 Z 1 DSGVO enthält Art 6 Abs 1 DSGVO eine taxative Liste von sechs Erlaubnistatbeständen:

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

Art 9 Abs 2 DSGVO enthält die taxative Liste jener zehn Erlaubnistatbestände, auf welche die Verarbeitung besonderer Kategorien personenbezogener Daten[63] (kurz: sensibler Daten) gestützt werden kann.

- lit a – Die ausdrückliche Einwilligung der betroffenen Person;
- lit b – die Erforderlichkeit zur Erfüllung von Pflichten oder Ausübung von Rechten im Arbeits- und Sozialrecht;
- lit c – die Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines *Dritten*, ohne erteilter Einwilligung;
- lit d – interne Verarbeitung durch Organisationen ohne Gewinnerzielungsabsicht;
- lit e – die Verarbeitung von offensichtlich durch die betroffene Person selbst öffentlich gemachten Daten;

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

- lit f – die Erforderlichkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte;
- lit g – die Erforderlichkeit aus Gründen eines erheblichen öffentlichen Interesses;
- lit h – die Erforderlichkeit für Zwecke des Gesundheits- oder Sozialwesens;
- lit i – die Erforderlichkeit aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- lit j – die Erforderlichkeit für im öffentlichen Interesse liegende Archiv-, Forschungs- oder statistische Zwecke.

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

4.2.2 Nachweis der Identität laden und anzeigen

Die Datenverarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationale Rechtsgrundlage für die Anmeldung an der ID-Austria bilden die §§ 4 iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3, § 14a Abs 2 E-GovG und § 18 Abs 1 E-GovG.[64]

Die nationalen Rechtsgrundlagen für die Übermittlung und Anzeige von Vorname, Nachname, Geburtsdatum und Lichtbild bilden die §§ 4 Abs 5 und 4 Abs 6 E-GovG iVm §§ 4 ff E-ID-Verordnung. Vor der Übermittlung wird gemäß § 4 Abs 2 E-GovG die Einwilligung der betroffenen Person eingeholt. Grundlage für den Erlass der E-ID-Verordnung bilden die §§ 4a Abs 6, § 18 Abs 3 und 4 sowie § 25 Abs 3 E-GovG, wobei hinsichtlich des vorliegend einschlägigen § 4 E-ID-Verordnung § 18 Abs 4 E-GovG maßgeblich ist.

So kann gemäß § 4 Abs 2 lit c E-ID-Verordnung das aktuelle Lichtbild, ausgenommen das Lichtbild eines Reisepasses gemäß § 4a des Passgesetzes 1992, aus dem Identitätsdokumentenregister (IDR) an den E-ID-Inhaber übermittelt werden.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[65] aus:

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

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

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

[64] Siehe genauer Punk 4.2.3 der DSFA betreffend ID-Austria unter: https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 15.05.2024).

[65] ErläutRV 469 BlgNR 27. GP 3, 8.

In Abs. 4 soll klargestellt werden, dass es für die Übermittlung der für die Nutzung des E-ID-Systems offenstehenden Datenarten zusätzlich zu Abs. 1 einer diesbezüglichen Rechtsgrundlage im jeweiligen Materiengesetz bedarf. Mit der vorgeschlagenen Verordnungsermächtigung soll ermöglicht werden, dass der für die jeweilige Datenverarbeitung zuständige Bundesminister die für eine Übermittlung gemäß Abs. 1 in Betracht kommenden Datenarten mit Verordnung konkretisieren kann, wobei sich jedoch die Rechtsgrundlage für die Datenübermittlung bereits aus einer gesetzlichen Regelung ergeben muss. Für eine Übermittlung gemäß Abs. 1 kommen lediglich Identitätsdaten (z. B. Vor- und Familiennamen sowie Geburtsdatum), Informationen zu Berechtigungen eines Betroffenen (z. B. Daten eines Reisedokumentes) oder Umstände, die der Betroffene nachweisen möchte (z. B. Hauptwohnsitz) in Betracht. Der Bundesminister für Inneres könnte beispielsweise die aus dem ZMR für die Verwendung der Funktion E-ID zur Verfügung stehenden Datenarten, die gemäß § 16a Abs. 4 MeldeG an die Stammzahlenregisterbehörde zur Erfüllung der gesetzlich übertragenen Aufgabe in Abs. 1 übermittelt werden, durch Verordnung präzisieren."

4.2.3 Identität gegenüber Exekutivorganen nachweisen

Der allgemeine Betrieb des Systems stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationale Rechtsgrundlage stellt § 4 Abs 6 iVm § 18 Abs 1 Z 2 E-GovG.

Im Rahmen einer Überprüfung verarbeiten Sicherheitsorgane Identitätsdaten. Die Verarbeitung der Identitätsdaten, also die Aushändigung, wird hierbei durch Art 6 Abs 1 lit e DSGVO iVm § 4 Abs 6 iVm § 18 Abs 1 Z 2 E-GovG gestützt. Die Einschau in das ZMR und das ERnP stützt sich auf 16a Abs 4 MeldeG, die Einschau in das IDR auf 22b Abs 4 iVm 4a Passgesetz 1992.

Zu Zweckrichtung und Verhältnismäßigkeit führen die Materialien aus:[66]

Zu § 22b Abs. 4 PassG:

„§ 18 Abs. 1 E-GovG regelt die Übermittlung der personenbezogenen Daten eines Registers eines Verantwortlichen des öffentlichen Bereichs an die Stammzahlenregisterbehörde. Voraussetzung für diese Übermittlung ist die Zugänglichkeit eines solchen Registers für die Stammzahlenregisterbehörde, die durch eine Ermächtigung zur Übermittlung von personenbezogenen Daten in den jeweiligen Materiengesetzen und die technische Anbindung eines Registers sichergestellt wird. Vor diesem Hintergrund soll mit der vorgeschlagenen Regelung zum Zwecke des elektronischen Nachweises von personenbezogenen Daten mithilfe des E-ID eine Ermächtigung zur Datenübermittlung aus dem IDR an die Stammzahlenregisterbehörde vorgesehen werden."

Zu § 22b Abs. 4a PassG:

„Erfahrungen aus der Verwaltungspraxis haben gezeigt, dass es für Behörden im Einzelfall einen über die „Tätigkeit im Dienste der Strafrechtspflege" hinausgehenden Bedarf gibt, mithilfe einer Abfrage von Namen, Geburtsdatum und -ort, Lichtbild sowie Pass- oder Personalausweisnummer die Identität einer Person gesichert festzustellen. Einschränkend soll eine diesbezügliche Abfrage des IDR nur in Betracht

[66] ErläutRV 469 BlgNR 27. GP 10.

kommen, sofern dies der Erfüllung einer gesetzlich übertragenen Aufgabe dient, die sonst nicht oder nicht in der nach den Umständen gebotenen Zeit wahrzunehmen ist. Die gesetzlich übertragene Aufgabe kann insbesondere in der behördlichen Überprüfung einer mutmaßlich unrechtmäßig erfolgten Anmeldung eines Wohnsitzes liegen, anlässlich derer die Identität des Betroffenen festzustellen ist. Bei der Überprüfung von Scheinmeldungen kann mitunter eine hohe Dringlichkeit gegeben sein, da an die Hauptwohnsitzmeldung diverse Sozialleistungen geknüpft sind sowie der Hauptwohnsitz einen maßgeblichen Bezugspunkt für gerichtliche Aufenthaltsermittlungen, gerichtliche Exekutionen wegen Geldforderungen oder Ähnliches darstellt. Zudem stellt die Möglichkeit der Überprüfung und Feststellung der Identität das gelindere und somit verhältnismäßigere Mittel dar, um die Dauer einer etwaigen Anhaltung zur Identitätsfeststellung durch ein Organ des öffentlichen Sicherheitsdienstes möglichst gering zu halten Der Verweis auf Abs. 4 zweiter Satz soll sicherstellen, dass eine derartige automationsunterstützte Abfrage im Einzelfall nur anhand der in § 22a Abs. 3 erwähnten Suchkriterien (Namen, Geburtsdatum, Reisepass- oder Personalausweisnummer, Verfahrenszahl oder bPK) zulässig ist. Nachweis der Identität gegenüber Privaten vorweisen."

4.2.4 Nachweis der Identität gegenüber Privaten vorweisen

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

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

4.2.5 Nachweis der Identität aktualisieren

Die Verarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die Aktualisierung stützt sich als technisch gleichgelagerter Unterfall der Funktion „Nachweis der Identität laden und anzeigen" auf §§ 4 Abs 5 und 4 Abs 6 E-GovG iVm §§ 4 ff E-ID-Verordnung. Die Anmeldung an der ID-Austria stützt sich auf die §§ 4 iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG. Genauere Angaben sind Punkt 4.2.2 zu entnehmen.

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;[67] 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*"[68] 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.[69]

Sofern jedoch zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, führt dies zur sogenannten "*pluralistische*[n] *Kontrolle*"[70] 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*"[71] 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,[72] 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.[73]

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

- *Namen und Kontaktdaten aller Verantwortlichen*[74]

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

- *Zweck(e) der gemeinsamen Verarbeitung;*
- *Einflussnahme der jeweiligen Verantwortlichen bei der Entscheidung über Zwecke und Mittel;*
- *Funktionale Beschreibung der gemeinsamen Verarbeitung, Aufgaben und Funktionen der jeweiligen Verantwortlichen sowie Offenlegung, wer welche Daten zu welchem Zweck verarbeitet;*
- *Beziehungen und Abhängigkeiten der wahrgenommenen Funktionen und der gemeinsam Verantwortlichen zueinander einschließlich allfälliger Datenübermittlungen zwischen den Verantwortlichen;*
- *Zuweisung eines Verantwortlichen zu jeder einzelnen sich aus der DSGVO ergebenden Pflicht für Verantwortliche; das Augenmerk sollte dabei insb auf die Betroffenenrechte gerichtet werden;*[75]
- *gegebenenfalls Benennung eines Verantwortlichen als zentrale Anlaufstelle nach Art 26 Abs 1 S 3*.[76]

An der jeweiligen Verarbeitung kann auch ein ***Auftragsverarbeiter*** mitwirken, der dem *Verantwortlichen* stets als *„verlängerter Arm"*[77] dient. Dies, da der *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, als rechtlich eigenständige und externe Organisation,[78] Datenverarbeitungstätigkeiten lediglich „im Auftrag" des *Verantwortlichen* durchzuführen hat. Daher kommt dem *Auftragsverarbeiter* grds keine Entscheidungsbefugnis hinsichtlich der Verarbeitungszwecke und (wesentlichen) -mittel zu.[79] 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.[80] Jedoch liegt die Entscheidungskompetenz über die „wesentlichen Mittel" der Verarbeitung stets beim *Verantwortlichen*.[81]

Die dem *Verantwortlichen* oder *Auftragsverarbeiter* unterstellten Personen gelten grds als ihnen *„zurechenbare Personen"*[82], da sie idR nur als *„Ausführungsorgan"* für den *Verantwortlichen* oder *Auftragsverarbeiter* tätig sind.[83] Dies gilt jedoch nur solange sie sich an die Vorgaben bzw vorab festgelegten Zwecke und Mittel der Verarbeitung halten.

---

[75] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[76] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41.
[77] *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter – was ändert sich mit der DSGVO? ZTR 2017, 59 (59).
[78] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 30.
[79] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 94.
[80] *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.
[81] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 17 f.
[82] 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.
[83] *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,[84] der zumindest ein „gewisses Maß an Eigenständigkeit“[85] aufzuweisen hat und dem personenbezogene Daten innerhalb einer Verarbeitungstätigkeit lediglich offengelegt werden.

Ferner gibt es auch die Rolle des „außenstehenden“[86] ***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.[87] Es kann daher jeder lebende[88] Mensch die Rolle der betroffenen Person einnehmen, unabhängig von einer spezifischen Voraussetzung iS eines bestimmten Alters oder Geisteszustands.[89]

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.[90] 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.[91]

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.[92]

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.[93] Daher richtet sich der grundrechtliche Schutz gem § 1 DSG auch auf

---

[84] 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,* (…).“

[85] 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.

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

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

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

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

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

[91] 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.*“

[92] 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.

[93] *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.

juristische Personen, wodurch nach systematischer Interpretation der Begriff „betroffene Personen“ in den einfachgesetzlichen Bestimmungen des DSG auch juristische Personen erfasst.[94] 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.[95]

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) Verantwortlichen

Basierend auf der bisherigen und maßgeblichen Rechtsprechung[96] 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.[97]
- 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.[98]
- Gemeinsame Verantwortlichkeit setzt nicht voraus, dass sämtliche Verantwortliche für dieselbe Verarbeitungstätigkeit einen (gemeinsamen) Zugang zu den betreffenden personenbezogenen Daten haben müssen.[99]
- 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

[94] *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.

[95] *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).

[96] 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*, E-CLI:EU:C:2019:629.

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

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

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

Folge.[100] Daher kann die Verantwortlichkeit bestimmter Verantwortlicher in verschiedenen Phasen und in unterschiedlichem Ausmaß ausgeprägt sein, wodurch der Grad der Verantwortlichkeit variieren kann.[101] Dabei kann man von einer qualitativ differenzierten Verantwortlichkeit sprechen. Charakteristisch hierfür ist, je größer die (Entscheidungs-)Macht eines *Verantwortlichen* über die Zwecke und Mittel der Verarbeitung ist, desto mehr Verantwortung geht damit einher bzw desto höher ist der Grad seiner Verantwortlichkeit.

- Das Organisieren, Koordinieren bzw „Ermuntern" zur Datenverarbeitung eines anderen *Verantwortlichen* (B) kann als eine auf Eigeninteresse beruhende Einflussnahme auf die Entscheidung über die Zwecke und Mittel der betreffenden Datenverarbeitung jenes *Verantwortlichen* (B) gedeutet werden, wodurch der einflussausübende Akteur (A) letztendlich an der Entscheidung über die Zwecke und Mittel der Verarbeitung faktisch mitwirkt, woraus die gemeinsame Verantwortlichkeit resultieren kann.[102]
- 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.[103]
- Für die Entscheidung über Zwecke und Mittel der Verarbeitung bedarf es keiner schriftlichen Anleitung oder Anweisung zur gemeinsamen Datenverarbeitung.[104]
- Eine gemeinsame Entscheidung über das Mittel der Verarbeitung (wie Social Plug-In[105]) 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.[106]
- 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.[107]

[100] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.
[101] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.
[102] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 68, 70 ff.
[103] Vgl EuGH C-25/17 VbR 2018/110 (202).
[104] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 67.
[105] 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.
[106] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77, 79.
[107] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 80 ff, 84.

- 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.[108]

4.3.3 Grundaspekte der Rollenverteilung im Zusammenhang mit dem digitalen Identitätsnachweis

Für die Rollenverteilung bezüglich der Funktion digitaler Identitätsnachweis, vor allem im Hinblick auf die Rolle des oder der *Verantwortlichen*, kommt dem Begriff der "*rechtlichen Verantwortlichkeit*"[109] maßgebliche Bedeutung zu. Denn dieser Beurteilungsaspekt geht aus Art 4 Z 7, 2. Halbsatz DSGVO hervor und demnach kann der *Verantwortliche* bzw die bestimmten Kriterien für seine Benennung im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden, sofern die Zwecke und Mittel der Verarbeitung durch das jeweilige Recht auch vorgegeben sind. So schlägt sich dieser Beurteilungsaspekt vor allem im öffentlichen Recht nieder, weshalb sowohl einem privaten als auch öffentlich-rechtlichen datenverarbeitenden Akteur kraft nationalem Recht bestimmte Aufgaben, die im öffentlichen Interesse liegen,[110] oder konkrete Verarbeitungstätigkeiten zugewiesen werden können, woraus sich basierend auf deren expliziter Zuständigkeit hierfür ihre rechtliche Verantwortlichkeit betreffend der mit den zugewiesenen Aufgaben einhergehenden Verarbeitung von personenbezogenen Daten ergeben kann.

In Anbetracht des Beurteilungsaspekts der rechtlichen Verantwortlichkeit sind vor allem die §§ 28 Z 1 iVm 7 Abs 2 iVm 4 Abs 8 iVm 4 Abs 6 EGovG iVm § 2 BMG einschlägig, welche die Zuständigkeit für die Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung für das Service und die Interaktion mit Bürgern und Unternehmen und sohin die rechtliche Verantwortlichkeit an das Bundeskanzleramt übertragen.[111] Hinsichtlich Ergänzungsregister liegt nach §§ 7 Abs 2 iVm 28 Z 2 E-GovG ebenfalls eine rechtliche Verantwortlichkeit des BKA vor und bildet eine vom digitalen Nachweis der Identität unabhängige Verarbeitungstätigkeit.

Die Materialien[112] führen erläuternd aus:

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

---

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

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

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

[111] Anlage zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG), BGBl I 1986/76 idF BGBl I 2024/44; siehe erläuternd: https://www.bundeskanzleramt.gv.at/agenda/digitalisierung/stammzahlenregisterbehoerde.html (abgerufen am 15.05.2024).

[112] ErläutRV 381 BlgNR 26. GP 2.

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“[113], zumal die vollumfängliche Verantwortung über eine Datenverarbeitung nur jener Akteur trägt, der über die Zwecke und Mittel der Verarbeitung entscheidet.[114] Diesbezüglich ist hervorzuheben, dass das BKA im Rahmen des gesetzlichen Auftrages den Betrieb der Schnittstelle zwischen Bürger*innen und ID Austria beauftragt und durch die federführende Beteiligung an deren Parametrierung auch wesentlichen faktischen Einfluss auf die Systemausgestaltung nimmt. Somit ist das BKA insgesamt als verantwortliche Stelle zu qualifizieren.

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

4.3.4 Nachweis der Identität laden und anzeigen

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BKA der BRZ GmbH (im Folgenden: BRZ) als *Auftragsverarbeiter*, welche im Auftrag des BKA die Schnittstelle zwischen ID Austria (bzw den einschlägigen Registern) und Nutzer*innen betreibt. Diese Verarbeitung erfolgt im Rahmen eines Vertragswerks, abgeschlossen zwischen der BRZ und der Republik Österreich, dessen Bestandteil auch ein Auftragsverarbeitungsvertrag nach Art 28 DSGVO ist.

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

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

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

Verantwortliche:

- BKA: Betrieb Funktion digitaler Identitätsnachweis, Betrieb Ergänzungsregister (ERnP)
- Meldebehörden: Zentrales Melderegister (ZMR)

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

- Passbehörden: Zentrales Identitätsdokumentenregister (IDR)

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Identitätsnachweis
- BMI: Betrieb Zentrales Melderegister (ZMR) und Identitätsdokumentenregister (IDR)

4.3.5 Identität gegenüber Exekutivorganen nachweisen

Da das BKA an diversen Stellen an den Datenverarbeitungen beteiligt ist, ist zu prüfen, ob dessen organisierende und koordinierende Tätigkeiten[115] eine gemeinsame Verantwortlichkeit mit den Melde- bzw. Passbehörden sowie dem BMI bzw den LPD oder den Gemeinden begründen. Konkret verantwortet das BKA die Parametrierung bzw Entwicklung der eAusweise-App, der GWK Check-App sowie der Ausweisplattform. Die Verarbeitung personenbezogener Daten durch Organe des Wachkörpers Bundespolizei bzw Organe der LPD im Rahmen einer Überprüfung liegt (wie bisher) im alleinigen Verantwortungs- und Gestaltungsbereich des BMI bzw der LPD, weshalb diese hinsichtlich dieser Verarbeitung insgesamt als verantwortliche Stellen zu qualifizieren sind.

Das Interesse des BKA an den im Zuge der konkreten Überprüfungsvorgänge anfallenden Daten erschöpft sich darin, dass es Rahmenbedingungen schafft, um Bürger*innen Dienste gemäß dem gesetzlichen Auftrag bereitzustellen. Es hat kein Interesse an den konkret fließenden Daten und auch keinen Einfluss darauf, ob Daten im konkreten Fall angefordert werden oder nicht. Sohin sind es die Organe des BMI bzw der LPD sowie der Gemeinde, die weitestgehend autonom darüber entscheiden, ob ein konkreter Datenfluss stattfindet oder nicht, wobei anzumerken ist, dass die Entscheidung, Identitätsdaten in digitaler Form vorzuweisen, bei der jeweiligen betroffenen Person selbst liegt, weil diese stets frei zwischen digitalem Nachweis der Identität und physischem Ausweis wählen kann. Umgekehrt eröffnet das BKA Bürger*innen unabhängig vom BMI, den LPD sowie den Gemeinden die Möglichkeit, Identitätsattribute digital vorzuweisen. BMI, LPD und Gemeinden haben hierbei keinen Einfluss auf die Parametrierung.

Zur Verantwortlichkeit der Melde- bzw Passbehörden siehe bereits Abschnitt 4.3.4.

Insgesamt liegt daher keine gemeinsame Verantwortlichkeit, sondern eine Übermittlung zwischen mehreren Verantwortlichen vor.

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BKA des BRZ als *Auftragsverarbeiter*.

Verantwortliche:

- BKA: Betrieb Funktion digitaler Identitätsnachweis, Betrieb GWK Check-App
- BMI bzw LPD: Organe des öffentlichen Sicherheitsdienstes ausgenommen Gemeindewachkörper
- Gemeinden: Gemeindewachkörper, Nutzung GWK Check-App
- Meldebehörden: Zentrales Melderegister (ZMR)

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

- Passbehörden: Zentrales Identitätsdokumentenregister (IDR)

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Identitätsnachweis, Betrieb GWK Check-App
- BMI: Betrieb Zentrales Melderegister (ZMR) und Identitätsdokumentenregister (IDR)

4.3.6 Nachweis der Identität gegenüber Privaten vorweisen

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

Die Verantwortlichkeit für den Betrieb der Funktion ist gleich gelagert wie bei „Nachweis der Identität laden und anzeigen“. Siehe genauer Abschnitt 4.3.4.

Die überprüfende Person verarbeitet im Zuge des Vorweisens Daten der Nutzer*in. Sie hat auch ein Interesse an der Datenverarbeitung, da diese eine Voraussetzung für eine Transaktion oder sonstige Interaktionen mit der Nutzer*in ist. Ob der organisierenden und koordinierenden Tätigkeiten[116] des BKA ist das Vorliegen einer gemeinsamen Verantwortlichkeit zwischen überprüfender Person und BKA zu erwägen. Die überprüfende Person entscheidet jedoch autonom, ob sie einen Prüfungsvorgang startet und verfolgt daneben eigenständige, auf konkrete Beziehungen zur Nutzer*in gerichtete Interessen. Das BKA hat weder unmittelbare noch mittelbare Interessen an den konkreten verarbeiteten Daten oder den Verarbeitungszwecken. Somit liegt auch hier keine gemeinsame Verantwortlichkeit vor.

Verantwortliche:

- BKA: Betrieb Funktion digitaler Identitätsnachweis
- Überprüfende Person: Überprüfung der Identitätsdaten

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Identitätsnachweis

4.3.7 Nachweis der Identität aktualisieren

Die Verantwortlichkeit ist gleich gelagert wie bei „Nachweis der Identität laden und anzeigen“. Siehe dazu Abschnitt 4.3.3.

Verantwortliche:

- BKA: Betrieb Funktion digitaler Identitätsnachweis

Auftragsverarbeiter:

- BRZ: Betrieb Funktion digitaler Identitätsnachweis

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

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.[117] 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.[118]

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

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

- Die betroffene Person kann frei entscheiden, ob sie den digitalen Nachweis der Identität oder ausschließlich physische Ausweise nutzt.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Identitätsnachweis vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten, die überdies direkt zwischen den Endgeräten ohne Einbeziehung eines Servers erfolgt.
- Die betroffene Person kann den digitalen Nachweis der Identität anzeigen lassen und kann so einschätzen, ob die darin enthaltenen Daten zweckdienlich sind.
- Der Prüfungsprozess kann jederzeit abgebrochen werden.
- Somit kann die betroffene Person selbst entscheiden, zu welchen Zwecken ihre personenbezogenen Daten im Zusammenhang mit digitalen Ausweisen verwendet werden und ob dies überhaupt der Fall sein soll, und kann die maximale Selbstbestimmung und Kontrolle über diese Vorgänge ausüben.

[117] Siehe zudem die primärrechtliche Grundlage in Art 8 Abs 2 EU-Grundrechte-Charta (GRC).
[118] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DSGVO (2018) 37.

- Die überprüfende Person kann Prüfvorgänge durchführen, ohne sich in der eAusweise-App an der ID-Austria anzumelden, oder überhaupt die eAusweis Check-App verwenden, sodass es zu keiner Verarbeitung ihrer personenbezogenen Daten kommt.

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

Nachweis der Identität laden und anzeigen

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

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Verschlüsselte Speicherung sowohl der Daten in der Ausweisplattform als auch der Daten auf dem Endgerät
- Grundsätzlich rein automatisierte Verarbeitung in der Ausweisplattform, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt
- Vor dem Laden des digitalen Identitätsnachweises ist eine Authentifizierung der jeweiligen Nutzer*in an der Plattform erforderlich, womit einem Zugriff bzw einer potenziell zweckwidrigen Verarbeitung durch andere Personen in diesem Zusammenhang entgegengewirkt wird.
- Reine Offline-Speicherung des digitalen Identitätsnachweises, womit auch einer potenziell zweckwidrigen, serverseitigen Verarbeitung vorgebeugt 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 Überprüfens von Ausweisen im System der Ausweisplattform nicht protokolliert.[119]
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen
- Die betroffene Person kann den Nachweis der Identität anzeigen lassen und kann so einschätzen, ob die darin enthaltenen Daten zweckdienlich sind.
- Nutzer*innen haben es selbst in der Hand, sich von der eAusweise-App abzumelden und haben volle Kontrolle über den dahinterliegenden Zweck. Dabei werden die in der App gespeicherten Identitätsdaten gelöscht.

Identität gegenüber Exekutivorganen nachweisen

Wie unter 3.3.2 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit das Vorweisen und Überprüfen des digitalen Identitätsnachweises gegenüber Exekutivorganen, wenn die Nutzer*in dies gegenüber dem Vorweisen des physischen Identitätsnachweises bevorzugt. Der dabei zu erzeugende QR-Code,

[119] https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

der hierzu eine Einsichtnahme in die Register (IDR/ZMR/ERnP) ermöglicht, enthält ua auch den MDS (Vorname, Nachname, Geburtsdatum). Dieser wäre zum Zweck des Abrufs der Ausweisdaten in den Registern nicht erforderlich und diese Daten wären ohnehin Teil der abgerufenen Ausweisdaten. Der Zweck dieser unmittelbaren Übermittlung des MDS im Wege des QR-Codes ist zum einen, dem überprüfenden Organ eine möglichst aktuelle Version dieser Daten bereitzustellen und zum anderen, dem Organ im Falle einer mangelnden Internetverbindung Vorname, Nachname und Geburtsdatum der Person, die sich soeben im Zuge der Überprüfung mit dem digitalen Nachweis der Identität ausweist, wie beim Vorweisen eines physischen Ausweises unmittelbar ersichtlich zu machen. Damit wird auch den gesetzlichen Anforderungen des § 22b PassG Rechnung getragen.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Nach allen dem BKA zum Zeitpunkt der Erstellung dieses Berichts vorliegenden Informationen ist eine Überprüfung des digitalen Nachweises der Identität für Exekutivorgane ausschließlich im gesetzlichen Rahmen vorgesehen und zulässig
- Für einen entsprechenden Zugriff auf die Register (IDR/ZMR/ERnP) ist eine Authentifizierung des jeweiligen Organs erforderlich und die entsprechende Serverkommunikation erfolgt verschlüsselt.
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen.
- Gesetzlich normierte Protokollierung von Zugriffen au die Register.

Nachweis der Identität gegenüber Privaten vorweisen

Wie unter 3.3.3 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit das Vorweisen und Überprüfen der Identitätsdaten.

Maßnahmen, um zweckwidriger Verarbeitung entgegenzuwirken:

- Das Vorweisen der Identitätsdaten findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.
- Verschlüsselte Verbindung der dabei involvierten Endgeräte
- Nutzer*innen können selbst darüber entscheiden, wem sie ihren digitalen Nachweis der Identität vorweisen und daher mittelbar auch bis zu einem gewissen Grad, zu welchem Zweck diese Daten durch Dritte verarbeitet werden.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Nachweis der Identität vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten.
- Bevor die überprüfte Person Daten an die prüfende Person übermittelt, muss die überprüfte Person aktive Schritte setzen. Der Prüfungsprozess kann jederzeit abgebrochen werden.

- Es werden dabei keine personenbezogenen Daten der *prüfenden* Person verarbeitet. Siehe zur Verarbeitung von Daten der *zu überprüfenden* Person die entsprechenden Ausführungen iZm dem Offline-Vorweisen des digitalen Nachweises der Identität gegenüber Privaten.

Nachweis der Identität aktualisieren

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

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

In praktischer Hinsicht heißt dies vor allem, dass die Risiken schon durch die Gestaltung der Architektur des Systems so gering wie möglich zu halten sind. Wenn sich aufgrund des Zwecks der Verarbeitung bspw nicht erklären lässt, warum personenbezogene Daten besser zentral als nur auf dem Endgerät gespeichert werden sollen, dann kann nur eine lokale Datenhaltung rechtmäßig sein. Wenn eine allenfalls unvermeidbare zentrale Datenhaltung auch mit einer Pseudonymisierung (Verschlüsselung) umgesetzt werden kann, dann ist eine unverschlüsselte Datenhaltung nicht rechtmäßig. Wenn eine längere Löschfrist das Risiko für die Nutzer*innen erhöht, ist die Frist für jeden Anwendungsfall so kurz wie nötig zu wählen.

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

- Bereits die Architektur des Systems der Ausweisplattform folgt dem datenschutzrechtlichen Prinzip Data Protection by Design („Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“) und damit auch dem Grundsatz der Datenminimierung; insbesondere werden die durch die betroffene Person auf eigene Initiative geladenen Identitätsdaten ausschließlich auf dem Endgerät der betroffenen Person gespeichert und das Vorweisen und Überprüfen des Nachweises erfolgt offline, dh ausschließlich auf den beiden verwendeten Endgeräten, und somit ohne dass dieser Vorgang eine Datenverarbeitung außerhalb der beiden verwendeten Endgeräte beinhaltet oder auslöst.

[120] Siehe auch ErwGr 39 DSGVO.

- Die Protokollierung ist hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt.[121]
- Daten werden gelöscht, wenn sie für ihren Zweck nicht mehr erforderlich sind; siehe dazu insbesondere auch Abschnitt 4.4.3 unten.
- Daten werden nur verarbeitet bzw übermittelt, soweit dies für den jeweiligen Zweck erforderlich ist.
- Zugriffsrechte bestehen nur im erforderlichen Ausmaß.
- Die Aktualisierung von Identitätsdaten erfolgt niemals automatisch, sondern nur auf Initiative der betroffenen Person, was auch der Systematik des § 4 Abs 6 E-GovG entspricht.

In Bezug auf die Unterschiede zwischen der Umsetzung des Vorweisens des digitalen Identitätsnachweises gegenüber Exekutivorganen und Privaten sind folgende Erwägungen in Hinblick auf die Erforderlichkeit und den Grundsatz der Datenminimierung zu erwähnen:

- Die zur Prüfung befugten Organe haben bereits bisher Zugriff auf die Register (IDR/ZMR/ERnP). Dieser Zugriff unterliegt spezifischen Maßnahmen zum Schutze der Rechte und Freiheiten der Betroffenen. Der Nachweis gegenüber Exekutivorganen wurde daher dem bisherigen Vorgehen bei Einsichtnahme in diese Register nachgebildet, wobei im Fall des digitalen Identitätsnachweises die Information, von welcher Person Registerdaten abzurufen sind, vom Endgerät der betroffenen Person mittels QR-Code zum Endgerät des überprüfenden Organs übertragen wird.

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.[122]
- Sofern die Nutzer*in in der eAusweise-App “dieses Gerät abmelden” auswählt, werden jedenfalls alle entsprechenden Daten, die auf diesem Gerät gespeichert sind, gelöscht. Sofern es sich um das einzige bzw letzte Gerät handelt, das die Nutzer*in im Zusammenhang mit der eAusweise-App verwendet, werden zudem auch alle serverseitig in der entsprechenden Datenbank gespeicherten Daten gelöscht, andernfalls nur jene Daten, die in Bezug auf das jeweilige Gerät in jener Datenbank gespeichert sind.
- Im Zuge der Anmeldung vergebene Registrierungstoken werden zudem nach deren einmaliger Nutzung aus der entsprechenden Datenbank gelöscht.

[121] https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).
[122] https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024).

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 des Registrierungsprozesses zusätzlich zu den zu akzeptierenden Nutzungsbedingungen die Datenschutzerklärung präsentiert. Diese kann auch danach jederzeit in der App im Bereich „Mein Profil" abgerufen werden.

Außerdem steht den Nutzer*innen im Zusammenhang mit der jedenfalls im Zuge des Registrierungsprozesses einmalig durchzuführenden Identitätsbestätigung der Zugriff auf die Datenschutzerklärung der dafür benötigten ID Austria mittels Link[123] 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 BKA[124] 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.[125]

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 BKA[126] angegeben.

---

[123] Zum Zeitpunkt der Erstellung des Berichts unter https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html (abgerufen am 15.05.2024)..
[124] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 15.05.2024).
[125] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 15.05.2024).
[126] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 15.05.2024).

Ebenfalls kommt Betroffenen unter den in Art 17 DSGVO beschriebenen Voraussetzungen das Recht zu, vom *Verantwortlichen* die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Voraussetzungen sehen ein 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 BKA[127] die erforderlichen Kontaktmöglichkeiten angegeben.

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[128] als auch auf der entsprechenden Website des BKA[129] 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.[130]

4.6 Datenübermittlung in Drittländer (oder an internationale Organisationen)

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

4.7 Rat des Datenschutzbeauftragten und Standpunkt der Betroffenen

Nach Art 35 Abs 2 DSGVO hat der Verantwortliche bei Durchführung einer DSFA den Rat des Datenschutzbeauftragten einzuholen. Ob der Rat des Datenschutzbeauftragten verpflichtend einzuholen ist und inwiefern dem eingeholten Rat des Datenschutzbeauftragten zu folgen ist, wird in der Literatur uneinheitlich kommentiert: *Trieb* geht bspw davon aus, dass die DSGVO keine solche Pflicht statuiert;[131] *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.[132] Falls der Verantwortliche mit dem vom Datenschutzbeauftragten ein-

[127] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 15.05.2024).
[128] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html (abgerufen am 15.05.2024).
[129] Siehe https://www.bmf.gv.at/public/datenschutz.html (abgerufen am 15.05.2024).
[130] 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 15.05.2024).
[131] Vgl *Trieb*, in *Knyrim*, DatKomm Art 35 Rz 124.
[132] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 18.

geholten 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.[133]

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.[134] Die Bestimmung des Abs 9 schafft grundsätzlich die Möglichkeit, die individuelle Meinung einzelner Betroffener in Erfahrung zu bringen.[135] Alternativ können auch deren "*Vertreter*" herangezogen werden, wobei in erster Linie an verschiedene Interessensvertretungen, Betriebsräte oder Verbraucherschutzverbände zu denken ist; der Standpunkt dieser Einrichtungen sollte insb dann berücksichtigt werden, wenn die beabsichtigte Datenverarbeitung eine große Zahl betroffener Personen erfasst, deren Interessen der jeweilige Verband oder die jeweilige Stellte vertritt.[136] Auch diese Regelung lässt in mehrfacher Hinsicht Deutungsspielräume offen.[137] 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.[138] Eine bedingungslose Verpflichtung für Verantwortliche zur Einholung wird auf Basis dieser Bestimmung nicht unterstellt werden können;[139] die jeweilige Vorgehensweise ist jedoch zu dokumentieren bzw zu begründen.[140]

Beginnend mit intensivem fachlichen Austausch zur Fertigstellung der Datenschutz-Folgenabschätzung betreffend den digitalen Führerschein wurde ein effektiver Prozess für den Dialog zwischen der Zivilgesellschaft und der Forschung unter dem Verantwortlichen angestoßen. Vor dem Übergang zum operativen Echtbetrieb einer Anwendung[141] stellt der Verantwortliche Vertretern der Zivilgesellschaft und der Forschung einschlägige Dokumentationen zur Verfügung und lädt zur ausführlichen Diskussion

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

[134] 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.

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

[136] 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.

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

[138] 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.

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

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

[141] Bisher zum digitalen Führerschein, zum digitalen Zulassungsschein, zu Ausweisplattform Phase 2 und dem digitalen Nachweis des Alters.

ein. Dieses bewährte Vorgehen wird ebenfalls im Kontext der Einführung des digitalen Identitätsnachweises beibehalten.

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 untersteht das relevante Verwaltungshandeln der parlamentarischen Kontrolle und damit der Kontrolle der Vertreter des Volkes. Diese Kontrollmöglichkeit wird auch regelmäßig im Rahmen von parlamentarischen Anfragen hinsichtlich Ausweisplattform ausgeübt (siehe insb 10037/AB, 13320/AB).

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,[142] 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.[143] 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.[144] 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

[142] 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.

[143] 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.

[144] 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.

– wenn die Verarbeitung eine große Menge an personenbezogenen Daten und eine große Anzahl von Personen betrifft.

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.[145]

Unter Bezugnahme auf die vorgenommene Abgrenzung des Gegenstandes der vorliegenden DSFA (siehe in Kapitel 3) ist darauf hinzuweisen, dass im Folgenden insbesondere eine Beurteilung möglicher Risiken in der Einflusssphäre des BKA vorgenommen werden kann. So sind Risiken in der Sphäre jener Verantwortlichen, denen die betroffenen Personen digitale Aus- oder Nachweise vorweisen, weder in der datenschutzrechtlichen Verantwortlichkeit des BKA noch durch das BKA in der Praxis beherrschbar. Soweit bestimmte Risiken aber vorhersehbar sind, wurden diese im Rahmen der Risikobeurteilung berücksichtigt und wenn möglich, auch mit Maßnahmen dieses Systems adressiert.

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.[146]

[145] https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf (abgerufen am 15.05.2024).

[146] 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.[147] Darüber hinaus wurde Anleihe am Risk Assessment-Leitfaden des deutschen Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom),[148] sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Fraunhofer-Institutes für System- und Innovationsforschung genommen.[149]

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.[150]

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[151]

- 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.[152]

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.[153]

In den methodischen Ausführungen des Fraunhofer-Instituts werden für die generelle Erfassung eines Risikoszenarios wiederum die folgenden übergeordneten Fragen aufgeworfen:[154]

- Welche Schäden können für betroffene Personen auf Grundlage der geplanten Datenverarbeitung auftreten?

---

147 https://www.iso.org/standard/65694.html (abgerufen am 15.05.2024).

148 Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung, https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf (abgerufen am 15.05.2024).

149 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.

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

151 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.

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

153 Vgl ErwGr 83 DSGVO.

154 Vgl *Martin et al*, Datenschutz-Folgenabschätzung 43.

- Durch welche Handlungen bzw Umstände kann es zum Eintritt der jeweiligen Schadensereignisse kommen? Welche Akteure bzw (nicht-menschliche) Risikoquellen sind dabei wie involviert?
- Welche Abhilfemaßnahmen sind bereits implementiert bzw geplant?[155]

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:[156]

- **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“*.[157]

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

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

[156] 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.

[157] Vgl ErwGr 76 DSGVO.

Risikobeurteilung (Template)

1) Risikoidentifikation	**Risikobeschreibung**
	Beschreibung und kurze deskriptive Erläuterung des Szenarios, Nennung beteiligter Akteure und Personen,[158] 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“?

[158] 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 15.05.2024) 30 f.

	Dies dürfte regelmäßig in der Nichteinhaltung der Datenschutzgrundsätze (Art 5 Abs 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art 12 bis 22 DSGVO) oder anderer Verstöße gegen die DSGVO (wie zB einem ungerechtfertigten Datentransfer ins Ausland) liegen.[159] **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?[160] **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 Pri-

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

	vatsphäre (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)

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.[161] Die Risikoidentifikation bezieht sich auf diese

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

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.[162] Im Zuge der Risikobeurteilung sind die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu eruieren.[163] Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annahmen zur angemessenen Einstufung des identifizierten Risikoszenarios.[164]

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit[165]

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[166]

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.

[162] 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.

[163] Vgl ErwGr 75 und 76 DSGVO.

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

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

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

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in einer Risikomatrix verortet. Der Risikograd ist methodisch definiert als das Produkt von Eintrittswahrscheinlichkeit und Schadensausmaß.[167] 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,[168] wie in der nachfolgenden Risikomatrix dargestellt.

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.[169]

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.[170] 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,

[167] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 8 (9).
[168] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46; vgl hierzu weiterführend auch *Friedewald et al*, Datenschutz-Folgenabschätzung 31.
[169] Vgl *Friedewald et al*, Datenschutz-Folgenabschätzung 31.
[170] Siehe Art 35 Abs 7 lit d DSGVO; vgl *Martin et al*, Datenschutz-Folgenabschätzung 38.

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.[171]

Die in Art 35 Abs 7 lit d DSGVO genannte „Bewältigung" wird gemeinhin auch als „Reduktion" bzw „Eindämmung" verstanden.[172] Durch die Maßnahmen sollten zumindest alle als „hoch" bewerteten Risiken so weit reduziert werden, dass sie nur noch als „normal" einzustufen sind.[173] Dabei ist es nicht zwangsläufig notwendig, zusätzliche Maßnahmen zu implementieren; mitunter kann es auch sinnvoller sein, bestehende Maßnahmen zu stärken.[174]

In Art 32 Abs 1 DSGVO werden zur Gewährleistung eines angemessenen Schutzniveaus folgende Optionen bzw Maßnahmen der Risikobehandlung angeführt:[175]

- 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.[176] Die verschiedenen Maßnahmen, Garantien und Verfahren sollen letztlich den Schutz personenbezogener Daten sicherstellen und die Einhaltung der Bestimmungen dieser Verordnung nachweisen.[177]

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.

---

[171] Vgl ErwGr 78 DSGVO.
[172] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46.
[173] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 47.
[174] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 48.
[175] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 33 f.
[176] 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.
[177] Vgl ErwGr 90 DSGVO.

Abschließend geht es in einer generellen Zusammenschau um die Feststellung des verbleibenden Restrisikos und der damit verbundenen weiteren Risikobehandlung durch den *Verantwortlichen*.[178] 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.[179] 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.[180]

[178] 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.

[179] 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.

[180] 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.[181] Dabei ist zu beachten, dass konsequent die Perspektive der Betroffenen eingenommen wird. Die Folgen- und Risikoabschätzung ist als Prozess zu verstehen und laufend an die tatsächlichen Gegebenheiten und Entwicklungen anzupassen und zu aktualisieren.

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

5.2.1 Unfreiwillige Nutzung des digitalen Nachweises der Identität

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person möchte zwar den digitalen Nachweis der Identität nicht nutzen, installiert und verwendet diesen aber dennoch, weil sie entweder durch äußere Umstände einem Druck ausgesetzt ist, diesen zu nutzen, oder der (irrigen) Annahme unterliegt, ihn künftig beim Bezug bestimmter Leistungen (zB Erstellung von Bankkonten) in digitaler Form vorweisen zu müssen. Insbesondere falls die Nutzung des digitalen Identitätsnachweises künftig weite Verbreitung finden sollte, kann es zu Formen sozialen Drucks oder faktischen Zwangs zur Nutzung des digitalen Identitätsnachweises anstelle eines physischen Ausweises kommen. Dies unter der Annahme, dass sich der Auslesevorgang für die überprüfende Person unter Umständen einfacher gestaltet und weiters angesichts der Tatsache, dass die Fälschungssicherheit höher ist. So könnte es beim digitalen Nachweis der Identität der prüfenden Person (bei Nutzung eigener spezifischer Applikationen) leichter fallen, Daten automatisiert zu verarbeiten und Querverbindungen zwischen Nachweisen anzustellen als es bisher beim physischen Ausweis der Fall war. Sollte sich dies manifestieren, würde dies eine Zunahme der Verarbeitung personenbezogener Daten und Intensivierung des damit in Verbindung stehenden Grundrechtseingriffs bedeuten.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Entscheidungsträger*innen des *Verantwortlichen* • Interne Mitarbeiter*innen • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache

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

	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu entsprechendem Druck zur Nutzung der Ausweis-Apps • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer ungewollten bzw unrechtmäßigen Datenverarbeitung. • Einschränkung der informationellen Selbstbestimmung • Unpräzise oder fehlende Kommunikation durch den *Verantwortlichen* oder andere zuständige Stellen, dass analoge Ausweise weiterhin uneingeschränkt genutzt werden können • Größere Zahl von Privaten, insbesondere Unternehmen, deren Verhalten zu entsprechenden Drucksituationen führt und welche Nachweisdaten mit Applikationen erheben, welche über den Funktionsumfang der eAusweise-App hinausgehen. • Politische Entscheidungen und/oder die fortschreitende Verwaltungsdigitalisierung könnten zu einem faktischen Zwang zur Verwendung der eAusweise-App führen, falls ohne diese bestimmte Verwaltungsprozesse unverhältnismäßig erschwert oder gar nicht mehr möglich sind.
	Möglicher Schaden für die betroffenen Personen
	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. • Unfreiwillige oder auch bloß unreflektierte Herausgabe der Identität oder einzelner Attribute, weil diese bei bestimmten Diensten nunmehr verlangt werden, da die eAusweise-App deren komfortable Herausgabe ermöglicht • Verringerte Anonymität und verstärktes Hinterlassen personenbezogener Datenspuren im Alltagsleben • Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung der eAusweise-App bzw des digitalen Nachweises der Identität 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**
	Wesentlich (3)	Maximal (4)	Hoch (12)

		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 Risiken.	

3) Maßnahmen	**Bestehende Maßnahmen**
	• Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Stringente Außenkommunikation hinsichtlich Nutzungsmöglichkeiten physischer Ausweise • Das Datenschutzrecht untersagt das Verlangen bestimmter Attribute, wenn dies für den jeweiligen Zweck nicht erforderlich ist (insb Art 5 Abs 1 DSGVO, Grundsatz der Rechtmäßigkeit, Grundsatz der Zweckbindung und Grundsatz der Datenminimierung). • Weder existiert nach aktueller Gesetzeslage irgendein Anwendungsfall, der die Verwendung eines digitalen Nachweises oder derzeit konkret des digitalen Identitätsnachweises als einzig zulässige Variante für die Bürger*in festlegt, noch ist nach derzeitigem Wissensstand ein solcher angedacht oder gar in Planung. In der Außenkommunikation wird das BKA deutlich auf diesen Umstand hinweisen. • Aufgrund der datensparsamen Konzeption und Implementierung des digitalen Nachweises der Identität, insbesondere durch die datensparsame Möglichkeit der offline-Speicherung und Nutzung, wird dieses Risiko weitgehend entschärft. Dies betrifft vor allem auch den Aspekt einer möglichen personenbezogenen Weiterverarbeitung der Daten, da Daten zur Herstellung des Personenbezugs nicht von der Übermittlung umfasst sind. • Möglichkeit den digitalen Altersnachweis zu nutzen • Existenz des anonymen Nachweises des Alters • *Geplante* Maßnahme: Implementierung der Steuerung der Auslesbarkeits- bzw Überprüfungsmöglichkeiten durch technische Vertrauensmechanismen (Verifizierung der prüfenden Applikation)

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

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

5.2.2 Diskriminierung aufgrund von Nicht-Nutzung des digitalen Nachweises der Identität

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person verwendet den digitalen Identitätsnachweis bewusst nicht, wobei dies verschiedene Gründe haben kann, zB mangelnde digitale Affinität, Mangel eines Smartphones mit Biometrie-Funktion, Ablehnung der eAusweise-App und/oder der ID Austria, Ablehnung der Nutzung der Biometrie-Funktion des Smartphones, insbesondere aus Datenschutzgründen etc, und erleidet dadurch Nachteile. Durch die potenziell weitverbreitete Verwendung des Systems und etwa des digitalen Identitätsnachweises könnte es uU zu Situationen kommen, in denen insb private *Verantwortliche* auf das Vorweisen eines digitalen Nachweises bestehen, insb weil im Vergleich dazu das Auslesen für die überprüfende Person leichter und die Fälschungssicherheit höher ist. Dadurch würden potenziell Personen diskriminiert, die den digitalen Nachweis der Identität bewusst nicht verwenden oder nicht die entsprechend vorausgesetzte digitale Infrastruktur bzw auch etwa eine ID Austria haben (wollen oder können).
	Risikoquelle
	Interne / Externe menschliche Quellen: • Entscheidungsträger*innen des *Verantwortlichen* • Interne Mitarbeiter*innen • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache
	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu weitverbreiteter Nutzung der eAusweise-App bzw des digitalen Nachweises der Identität • Einschränkung der informationellen Selbstbestimmung • Verhalten privater Anbieter (zB Banken), das zu entsprechenden Situationen führt • Politische Entscheidungen und/oder die fortschreitende Verwaltungsdigitalisierung könnten zu einer Diskriminierung bei Nicht-Nutzung der eAusweise-App führen, falls künftig ohne diese bestimmte Verwaltungsprozesse erschwert oder gar nicht mehr möglich sind. • Unpräzise oder fehlende Kommunikation durch den *Verantwortlichen* oder andere zuständige Stellen, dass physische Ausweise weiterhin uneingeschränkt genutzt werden können
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden:

	• Möglicher Ausschluss von system- oder alltagsrelevanten Diensten, womit auch finanzielle Schäden verbunden sein könnten (zB höherer Warenpreis soweit ein niedrigerer Warenpreis den digitalen Nachweis der Identität voraussetzt) **Immaterielle Schäden:** • Einschränkungen in Teilen der (zB privaten) Lebensführung • Einschränkungen in der Nutzung von Diensten aufgrund der Ablehnung, die eAusweise-App bzw den digitalen Nachweis der Identität zu nutzen

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

3) Maßnahmen	**Bestehende Maßnahmen**
	• Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Verwendung von physischen Ausweisen weiterhin möglich. • Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Identitätsnachweises als moderne Inklusionsvariante eine erleichterte und datensparsame Variante und somit gleichsam als Gegenteil eines Diskriminierungsinstruments konzipiert ist • Hardwarenotwendigkeit ergibt sich aus der Konzeption des Prüfprozesses • *Geplante* Maßnahme: Implementierung der Steuerung der Auslesbarkeits- bzw Überprüfungsmöglichkeiten durch technische Vertrauensmechanismen (Verifizierung der prüfenden Applikation)

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

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

1) Risikoidentifikation	**Risikobeschreibung**
	Eine unbefugte Person verschafft sich über das AWP-Backend Zugriff auf eines der dahinterliegenden Register. Über das AWP-Backend ist der Bezug von Daten aus dem IDR/ZMR/ERnP (über die ID-Austria) möglich, um Daten der jeweiligen Nutzer*innen beziehen zu können. Zumal es sich dabei um hochqualitative Daten handelt, könnte ein Interesse daran bestehen, unbefugter Weise darauf zuzugreifen und entsprechende Daten (§ 22b Abs 1 und Abs 4 iVm § 22a Abs 1 Passgesetz 1992 iVm § 18 Abs 1 E-GovG) anderer Personen zu akquirieren.
	Risikoquelle
	Interne /Externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) **Interne / externe technische Quellen:** • Softwarefehler
	Risikoursache
	• Unbefugte bzw unrechtmäßige Verarbeitung der in IDR/ZMR/ERnP enthaltenen Daten
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden • wirtschaftliche oder gesellschaftliche Nachteile durch Bekanntgabe der Wohnadresse (Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte) • gesellschaftliche Nachteile

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

3) Maßnahmen	Bestehende Maßnahmen
	• Über das AWP-Backend besteht kein direkter Zugriff auf IDR/ZMR/ERnP. Die Daten werden standardmäßig über die ID Austria ausgeliefert. • Die Schnittstelle zur ID-Austria durch die AWP benötigt zwingend das verschlüsselte bPK der der jeweiligen Bürger*in.

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

5.2.4 Erhöhter Druck sich gegenüber Exekutivorganen auszuweisen

1) Risikoidentifikation	Risikobeschreibung
	Für österreichische Staatsbürger*innen gibt es im Inland grundsätzlich keine allgemeine Pflicht, in der Öffentlichkeit stets einen Ausweis mitzuführen, um sich jederzeit ausweisen zu können.[182] Eine weite Verbreitung digitaler Ausweise könnte dazu führen, dass man – anders als bisher – stets annehmen kann, dass eine Person sich ausweisen kann, weil nahezu alle Personen ein Smartphone besitzen, dieses iaR mitführen und somit die Möglichkeit haben, sich jederzeit digital auszuweisen. Diese potenzielle erhöhte Verfügbarkeit von Ausweisen könnte zu einer allgemeinen Ausweitung von Ausweiskontrollen führen.
	Risikoquelle
	Externe menschliche und strukturelle Quellen: • Externe Entscheidungsträger*innen
	Risikoursache
	• Allgemeine Erwartungshaltung, dass Betroffene sich jederzeit ausweisen können, möglicherweise ohne Problembewusstsein

[182] Vgl etwa VwGH 29. 6. 2000, 96/01/1071 mit Verweis auf *Wiederin*, Einführung in das Sicherheitspolizeirecht Rz 456; LVwG Steiermark 11. 4. 2019, LVwG 20.3-3050/2018 mwN; LVwG Salzburg 16. 1. 2018, LVwG 405-12/18/1/17-2018; vgl allerdings in Bezug auf "Fremde" einerseits § 32 Abs 2 Fremdenpolizeigesetz 2005 BGBl I 2005/100; vgl außerdem etwa bzgl § 35 Abs 1 Z 6 SPG auch VwGH 25. 2. 2014, 2012/01/0149.

	• Die einzelnen Kontrollhandlungen erscheinen möglicherweise gerechtfertigt oder problemlos, die Summe dieser Handlungen ergeben jedoch den erhöhten Kontrolldruck.
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: • Einschränkungen in Teilen der (zB privaten) Lebensführung • Verarbeitung personenbezogener Daten – zulässige wie unzulässige – gegen den Willen der betroffenen Person in einem Ausmaß, welches in der Vergangenheit offenbar nicht erforderlich war • Verringerte Anonymität und verstärktes Hinterlassen personenbezogener Datenspuren im Alltagsleben

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Eingeschränkt (2)	Wesentlich (3)	Normal (6)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Aufnahme entsprechender Hinweise in Schulungsunterlagen hinsichtlich der Nutzung des digitalen Nachweises der Identität • Eine Überprüfung des digitalen Nachweises der Identität für Exekutivorgane ausschließlich im gesetzlichen Rahmen vorgesehen und zulässig.

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

5.2.5 Protokollierung zu vieler personenbezogener Daten

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass im Zuge der Verwendung der eAusweise-App auf der Ebene des IDR/ZMR/ERnP mehr personenbezogene Daten protokolliert werden, als dies zur Erfüllung der Anforderungen des Datenschutzrechts und zur Erfüllung aller anderen legitimen Anforderungen unbedingt erforderlich ist. Damit ist stets das Risiko verbunden, dass diese Protokolldaten offengelegt bzw zweckwidrig verarbeitet

	werden und deshalb bekannt wird, an welchen Stellen Betroffene ihren digitalen Nachweis verwendet haben.
	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 **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: Keine eingriffsintensiven Datenkategorien betroffen.	Normal (6)

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es hier architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.	

	• Die Protokollierung unterliegt klaren gesetzlichen Regeln.

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

5.2.6 Missbräuchliche Verwendung von Protokolldaten

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass Protokolldaten auf der Ebene des IDR/ZMR/ERnP offengelegt bzw zweckwidrig verarbeitet werden und deshalb insbesondere bekannt wird, an welchen Stellen Betroffene ihren digitalen Nachweis verwendet haben.
	Risikoquelle
	Interne/externe menschliche Quellen: • 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)	Normal (9)

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Nachweises findet offline statt. Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es hier architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. • Die Protokollierung unterliegt klaren gesetzlichen Regeln.	

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	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)

5.2.7 Unbefugte Verwendung der GWK Check-App

1) Risikoidentifikation	**Risikobeschreibung**
	Eine unbefugte Person verwendet die GWK Check-App, um der betroffenen Person zu suggerieren, sie sei ein befugtes Exekutivorgan. Kriminelle könnten aus verschiedenen Gründen versuchen, sich als Exekutivorgane auszugeben, wodurch betroffenen Personen Nachteile drohen könnten. Durch die Verwendung einer offiziellen Prüf-App beim Nachweis der Identität - in Verbindung mit anderen Täuschungsmaßnahmen, wie insbesondere dem Tragen einer Uniform - könnte der Eindruck erhärtet werden, dass es sich um ein dazu befugtes Organ handelt. Dieses Risiko besteht analog auch für jede andere App, die von Exekutivorganen zur Überprüfung des digitalen Identitätsnachweises verwendet werden kann. Jede solche App muss daher ebenfalls mindestens die unten angeführten Maßnahmen erfüllen.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Cyberkriminelle (Hacker/Schadsoftware) **Interne / externe technische Quellen:** • Softwarefehler
	Risikoursache
	• Installation und Verwendung der GWK Check-App durch Unbefugte • Vortäuschung, dass es sich bei der überprüfenden Person um ein Exekutivorgan handelt • Unbefugte Verarbeitung von Identitätsdaten der betroffenen Person
	Möglicher Schaden für die betroffenen Personen

	Materielle Schäden • Finanzieller Verlust aufgrund Zwangslange durch vermeintliche Befugnisse des vermeintlichen Exekutivorgans **Immaterielle Schäden** • Verletzung der Privatsphäre • Zwangslange durch vermeintliche Befugnisse des vermeintlichen Exekutivorgans

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Eingeschränkt (2)	Wesentlich (3)	Normal (6)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Personenbezogenes Login der Organe in die GWK Check-App und somit Beschränkung der Möglichkeit, die GWK Check-App zu verwenden auf Mitarbeiter*innen der Gemeindewachkörper durch Authentifizierung • Protokollierung aller Zugriffe auf die Register • Verfolgung und Aufdeckung von entsprechenden Täuschungsfällen sowie aktive Aufklärung der Öffentlichkeit darüber (etwa über Erkennungsmerkmale „echter“ Exekutivorgane) • Sogar unter der Annahme, dass es gelingen sollte, eine scheinbar offizielle GWK Check-App nachzubauen, wäre über diese kein Zugriff auf die Register möglich, da die tatsächlich befugten Personen auf einer Whitelist verzeichnet sind, die diesen den Zugang ermöglicht.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Vernachlässigbar (1)	Wesentlich (3)	Normal (3)

5.2.8 Nichtverfügbarkeit des Systems

	Risikobeschreibung

1) Risikoidentifikation	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 bei einem physischen Ausweis. Soweit kein (physisches) Substitut mitgeführt wird, könnten sich in Einzelfällen unter Umständen verwaltungsrechtliche Folgen oder 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 Risikos wird zunächst durch das Vertrauen der Nutzer*innen auf die Datenverfügbarkeit ermöglicht, soweit sie in diesem Vertrauen davon absehen, physische Ausweise mitzuführen. • Das Risiko kann eintreten durch eine Fehlfunktion im Authentifizierungsvorgang, sodass die an sich berechtigte Person es nicht schafft, sich zu authentifizieren („false negative“). Auslöser dafür kann sein, dass der biometrische Faktor nicht einsatzbereit ist oder nicht korrekt erkannt wird. Das kann zB verursacht werden durch: o Fehlfunktion in der Biometrie-Komponente des Smartphones (dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemherstellern) o Die Biometriekomponente steht bei einer ganzen Gerätegeneration nicht mehr zur Verfügung, weil sie aufgrund einer dokumentierten Kompromittierung deaktiviert werden musste

	(dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemherstellern). ○ Geringfügig geänderte physische Merkmale der Nutzer*in, durch Verletzungen, Hautprobleme etc Neben dieser spezifischen Ursache kann das Verfügbarkeitsrisiko auch durch viele verschiedene andere Ursachen (insb Komponenten der ID Austria, Ausweisplattform, Register, Endgeräte) ausgelöst werden. Zu beachten sind vor allem Systemteile, die vielleicht nicht als kritisch wahrgenommen werden, deren Ausfall aber trotzdem zur Nichtverfügbarkeit des Gesamtsystems führen kann. • Aktualisierungsdatum wird angezeigt • Vor Ablauf der Gültigkeit eines Nachweises der Identität wird die Nutzer*in durch die Applikation erinnert • Transparente, leicht erreichbare Informationserteilung durch den Verantwortlichen • Stringente FAQs
	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:** • Gesellschaftliche Nachteile • Verweigerung eines Zugangs oder Einlasses, weil sich die betroffene Person nicht ausweisen kann

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Maximal (4) Kommentar: Bei entsprechender Verbreitung sind durch Endgeräte bedingte Risikoeintritte sehr wahrscheinlich.	Eingeschränkt (2) Kommentar: Der schnellere Zugang zu Leistungen oder der Einlass kann (temporär) verwehrt sein, ebenso der Abschluss verwaltungsrechtlicher Vorgänge im Einzelfall.	Normal (8)

3) Maßnahmen	Bestehende Maßnahmen
	• Physische Ausweise können weiterhin diskriminierungsfrei in allen Lebenslagen verwendet werden. Unterstützung bzw Dokumentation (zB FAQ) bzgl Hinterlegung neuer biometrischer Daten am Endgerät. • Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Nachweises der Identität als moderne Inklusionsvariante und somit gleichsam als Gegenteil eines Einschränkungsinstruments konzipiert ist. • Das Vorweisen des digitalen Identitätsnachweises läuft offline ab und ist nicht von der Verfügbarkeit von Serverarchitektur abhängig.

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

5.2.9 Vertrauen auf die umfassende Einsetzbarkeit des digitalen Identitätsnachweises

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person verwendet den digitalen Nachweis der Identität bewusst und verlässt sich darauf, dass dessen Verwendung im Rechtsverkehr auf Akzeptanz stößt. Im Vertrauen darauf führt die betroffene Person keinen physischen Identitätsnachweis mit sich. Werden die Akzeptanzerwartungen etwa im Zuge des Abschlusses von Verträgen enttäuscht, kann es zu finanziellen Nachteilen kommen.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Sonstige Dritte (insb Anbieter*innen von Drittdiensten)
	Risikoursache
	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu weitverbreiteter Nutzung der eAusweise-App bzw des digitalen Identitätsnachweises, diese wird jedoch nicht von allen Marktteilnehmern mitgetragen. • Verhalten privater Anbieter (zB Banken), das zu entsprechenden Situationen führt. • Die betroffene Person verlässt sich (bewusst oder unbewusst ob des allgemein wahrgenommenen Digitalisierungsfortschritts) darauf, dass der digitale Identitätsnachweis in allen Lebenslagen auf Akzeptanz stößt.
	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:** • Gesellschaftliche Nachteile • Verweigerung des Zugangs oder Einlasses, weil sich die betroffene Person nicht ausweisen kann

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Wesentlich (3)	Eingeschränkt (2) Kommentar: Beibringen eines physischen Ausweises ist möglich, der Schaden ist daher überwindbar.	Normal (6)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Hinweis in den Nutzungsbedingungen, dass es sich beim digitalen Identitätsnachweis um ein Zusatzangebot an die Bürgerinnen und Bürger handelt, der digitale Identitätsnachweis jedoch weder dazu gedacht noch in der Lage ist, in allen erdenklichen Situationen als Ersatz für einen physischen Ausweis zu fungieren.

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

5.2.10 Vorweisen eines gefälschten digitalen Nachweises der Identität

1) Risikoidentifikation	**Risikobeschreibung**
	Es gelingt einem Angreifer, manipulierte Identitätsdaten via Bluetooth zu übermitteln, sodass die Überprüfungs-Funktion die Manipulation nicht erkennt und die Überprüfung des manipulierten Nachweises erfolgreich verläuft. Alternativ präsentiert der Angreifer gefälschte Identitätsdaten (zB als bearbeiteten Screenshot) und überzeugt die prüfende Person es bei einer Sichtprüfung zu belassen und keine Übermittlung der Identitätsdaten anzufordern.
	Risikoquelle
	Externe menschliche Quelle: • Sonstige Dritte
	Risikoursache
	Die Ursache kann eine Schwachstelle in der Funktion zur Erzeugung (insbesondere Signieren) und Übermittlung der Identitätsdaten via Bluetooth oder eine Schwachstelle in der Funktion zur Überprüfung der via Bluetooth empfangenen Identitätsdaten (insbesondere Signaturprüfung) sein.

	Daneben kann die Ursache in mangelndem Verständnis der prüfenden Person über die Funktion des digitalen Nachweises der Identität sein, was sie dazu veranlasst, die Sichtprüfung zu akzeptieren.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • wirtschaftliche oder gesellschaftliche Nachteile

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Maximal (4) Kommentar: Insbesondere Abschluss von Verträgen, oder das Setzen folgenreicher Handlungen im Vertrauen auf die Identität des Gegenübers.	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Die Identitätsdaten sind signiert und beim Überprüfen findet eine Signaturprüfung statt. Eine erfolgreiche Fälschung der Identitätsdaten wäre nur unter der Annahme der Korrumpierung der verwendeten Public Key Infrastructure des Systems der AWP denkbar, einschließlich der dazu erforderlichen Überwindung mannigfaltiger Sicherheitsmaßnahmen. • Beim Herzeigen der Identitätsdaten muss die Besitzer*in nachweisen, dass sie im Besitz des privaten Schlüssels ist, dessen öffentlicher Teil im Nachweis eingebunden ist. Dies bedeutet, dass die signierten Identitätsdaten alleine nicht für den Identitätsnachweis reichen, es muss auch der Beweis erbracht werden, dass man im Besitz des Schlüssels ist, der mit dem Nachweis verknüpft wird. • Prüfbarkeit des Lichtbildes durch die prüfende Person. • Die UI der eAusweise-App ist so gestaltet, dass Nutzer*innen zur Prüfung mittels Datenübertragung geleitet werden.

	• Hinweis in den Nutzungsbedingungen, dass die Sichtprüfung der Applikation der überprüften Person keine hinreichende Grundlage für Vertrauen in den Nachweis bildet

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Eingeschränkt (2)	Maximal (4) Kommentar: Insbesondere Abschluss von Verträgen, oder das Setzen folgenreicher Handlungen im Vertrauen auf die Identität des Gegenübers.	Normal (8)

5.2.11 Vorweisen nicht aktualisierter Identitätsdaten

1) Risikoidentifikation	**Risikobeschreibung**
	Die überprüfte Person kann auch nach faktischer Änderung von Identitätsdaten eine alte Version ihrer Identitätsdaten digital übermitteln. Dies könnte etwa bei Namensänderungen nach erfolgter Heirat der Fall sein. Es ist denkbar, dass die Nutzer*in vergisst, den digitalen Identitätsnachweis zu aktualisieren, oder dies vorsätzlich unterlässt, um bzgl ihrer Identitätsdaten zu täuschen.
	Risikoquelle
	Externe menschliche Quelle: • Nutzer*in
	Risikoursache
	Überprüfte Person übermittelt (veraltete) Identitätsdaten, obwohl sich wesentliche Umstände (Vorname oder Nachname) geändert haben.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Übervorteilung (zB bei Vertragsabschlüssen) (die überprüfende Person betreffend) • finanzieller Verlust (folgend aus der Identität der Vertragspartner*in oder der eigenen Identität) • Administrativer Aufwand im Zusammenhang mit nachträglicher Anpassung der Daten **Immaterielle Schäden** • gesellschaftliche Nachteile • Verarbeitung unrichtiger Daten

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Eingeschränkt (2)	Eingeschränkt (2) Kommentar: Möglichkeiten der Irreführung sind aufklärbar und kurzfristig. Insbesondere kann die prüfende Person eine Aktualisierung anfordern	Normal (4)

		und Schaden leicht überwinden.	

3) Maßnahmen	**Bestehende Maßnahmen**
	• Der überprüfenden Person wird der Zeitpunkt der letzten Aktualisierung angezeigt • Hinweis in den Nutzungsbedingungen, dass die Aktualität der Identitätsdaten zwangsläufig mit dem Zeitpunkt der letzten Aktualisierung einhergeht. • Gültigkeit des digitalen Identitätsnachweises ist technisch auf 3 Monate begrenzt.

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

5.2.12 Vorweisen des Nachweises einer anderen Person

1) Risikoidentifikation	**Risikobeschreibung**
	Ein Angreifer verwendet den eAusweise-App-Login einer anderen Person auf deren Endgerät oder einem anderen Endgerät, um einen - an sich nicht manipulierten - Nachweis dieser anderen Person vorzuweisen. Dies kann entweder mit Einverständnis der anderen Person oder gegen deren Willen erfolgen. Dem Angreifer gelingt es, sich als diese andere Person auszugeben, weil die überprüfende Person anhand des übermittelten Lichtbildes nicht erkennt, dass die Person auf dem Lichtbild nicht diejenige ist, die den Nachweis vorweist. Anzumerken ist: Zu einer Risikoerhöhung kommt es aufgrund des digitalen Nachweises der Identität (zB gegenüber einem physischen Identitätsnachweis) nur durch die (theoretische) Möglichkeit der Verwendung des eAusweise-App-Logins gegen den Willen der betroffenen Person, sodass der Angreifer nichts physisch entwenden muss. Die Problematik der Überprüfung des Gegenübers auf Übereinstimmung mit dem vorgewiesenen Foto besteht hingegen auch bei physischen Ausweisen und die Qualität der Fotowiedergabe in der App eAusweise wird demgegenüber deutlich höher sein.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Erfolgreicher Angriff auf ID Austria-Authentifizierung • Mangelnde Kontrolle über die Systeme der Smartphone-Hersteller und Betriebssystem-Hersteller • Strukturelle Probleme der Biometrie • Veraltete Gerätegenerationen: Viele Android- und Apple-Geräte, die im Umlauf sind, erhalten keine Sicherheitsupdates mehr, funktionieren aber noch einwandfrei und werden daher weiterverwendet; das Bewusstsein für diese Problematik ist bei vielen Nutzer*innen gering • Mangelnde Absicherung des Smartphones bzw leichtfertiges aus der Hand geben (zB unbeaufsichtigt lassen, zur Reparatur geben, etc) • Bewusste Weitergabe der elektronischen Identität durch den Betroffenen an den Angreifer
	Möglicher Schaden für die betroffenen Personen

	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Identitätsdiebstahl oder -betrug • Psychologische Schäden • Rufschädigung • Verletzung der Privatsphäre • wirtschaftliche oder gesellschaftliche Nachteile

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3) Kommentar: Das Gegenüber kann das Foto kontrollieren, es liegt in dessen alleiniger Verantwortung, dies auch tatsächlich zu tun; diesbzgl keine Risikoerhöhung gegenüber physischem Ausweis, bei dem dasselbe Problem besteht	Maximal (4)	Hoch (12)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Biometrische Authentifizierung beim Öffnen der eAusweise-App; dadurch wird das Vorweisen eines fremden digitalen Nachweises verglichen mit einem physischen Ausweis deutlich erschwert; dies ist auch gegen die bewusste Weitergabe durch rechtmäßige Ausweisinhaber*innen wirksam. • Der digitale Nachweis der Identität führt somit aufgrund der implementierten Sicherheitsmaßnahmen im Vergleich zur analogen Variante tatsächlich zu einer Reduzierung des Risikos des Vorweisens eines fremden Nachweises.

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

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

5.2.13 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.	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 BKA für den Betrieb von eGovernment-Infrastruktur.

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

5.2.14 Verwendung des digitalen Nachweises der Identität im Ausland

1) Risikoidentifikation	**Risikobeschreibung**
	Ausschließlich österreichischen Kontrollorganen kann durch das Vorweisen des digitalen Nachweises der Identität Dateneinsicht in die entsprechenden Register gewährt werden. Weiters handelt es sich nicht um ein Reisedokument. Es ist denkbar, dass Betroffene in Unkenntnis dessen dennoch den digitalen Nachweis der Identität anstatt eines physischen Ausweises bzw Reisedokuments im Ausland mitführen, weil sie vermeinen, damit über ein auch dort rechtlich ausreichendes Identitätsdokument bzw. Reisedokument zu verfügen.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Nutzer*in • Empfänger*innen
	Risikoursache
	• Unpräzise oder fehlende Kommunikation durch den *Verantwortlichen* oder andere zuständige Stellen. • Irrtum/Unkenntnis der betroffenen Person
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Erhalt einer behördlichen Strafe • Verwehrung des Bezugs von Leistungen (zB Check-in beim Hotel)

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Wesentlich (3) Kommentar: Im Ausland sind die Folgen des Nichtmitführens eines Identitäts- oder Reisedokuments nicht absehbar. Eine versuchte Verwendung als Personalausweis erscheint denkbar, als Reisepass jedoch unwahrscheinlich.	Normal (9)

3) Maßnahmen	Bestehende Maßnahmen
	• Transparente, leicht erreichbare Informationserteilung durch den *Verantwortlichen* • Stringente FAQs • Stringente Außenkommunikation hinsichtlich Nutzungsmöglichkeiten des digitalen Nachweises der Identität.

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

5.2.15 Auslesen des Nachweises ohne Rechtsgrundlage

1) Risikoidentifikation	Risikobeschreibung
	Der Überprüfende hat keine Rechtsgrundlage, die Daten der betroffenen Person zu verarbeiten (was das Überprüfen des Nachweises miteinschließt) und er dürfte daher von der betroffenen Person das Vorweisen eines Nachweises nicht verlangen. Zwar wird es stets zulässig sein, dass die betroffene Person ihren Nachweis freiwillig vorweist und dieser in der Folge auch durch die überprüfende Person gelesen wird, aber es ist sehr leicht möglich, dass diese Freiwilligkeit eingeschränkt ist (Drucksituation, Erforderlichkeit zum Erhalt einer Leistung, Aussicht auf eine Gegenleistung oÄ).[183] Eine Risikoerhöhung durch den digitalen Nachweis der Identität gegenüber einem physischen Ausweis ist nicht gegeben.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte • Cyberkriminelle
	Risikoursache
	• Bewusster, zielgerichteter Angriff

[183] Siehe in diesem Zusammenhang auch das Risiko 5.2.10 der DSFA-Ausweisplattform: https://www.oesterreich.gv.at/dam/jcr:fe86ad45-1e80-4e5b-9b25-13bd501e208d/DSFA-Ausweisplattform.pdf (abgerufen am 15.05.2024)

	• Druck auf die betroffene Person • Leichtgläubigkeit der betroffenen Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit digitalen Aus- oder Nachweisen • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Unbefugte Offenlegung von und Zugang zu Daten • Verarbeitung entgegen den Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	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**
	Maximal (4)	Eingeschränkt (2)	Normal (8)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Die betroffene Person muss beim Auslesen stets involviert sein. Insofern besteht keine Risikoerhöhung gegenüber einem physischen Ausweis. (Wie oben beschrieben bedeutet das aber nicht, dass stets Freiwilligkeit vorliegt.)

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

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

5.2.16 Bekanntwerden nicht erforderlicher Daten bei lediglich beabsichtigter Übermittlung des Geburtsdatums

1) Risikoidentifikation	**Risikobeschreibung**
	Der Überprüfende erhält beim Vorweisen des digitalen Nachweises der Identität Daten, die dieser unweigerlich enthält, die aber für den Zweck des jeweiligen Vorweisens nicht unbedingt erforderlich sind, wie etwa der Name im Zuge der (eigentlich vorgesehenen) Übermittlung des Geburtsdatums.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte, denen die Identitätsdaten vorgewiesen werden
	Risikoursache
	• Verarbeitung wider den Zweckbindungsgrundsatz • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • Verletzung der Privatsphäre • Ungerechtfertigte Beeinträchtigung von Rechten; durch Verarbeitung ohne ausreichende Rechtsgrundlage (zweckbezogene Einwilligung) • Bildung eines Profils (Erfassung von Daten aus verschiedenen Lebensbereichen) • Beeinträchtigung der informationellen Selbstbestimmung

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Es liegt im Ermessen der betroffenen Person, ob diese einen Ausweis zur Verfügung stellt.	Normal (6)

3) Maßnahmen	Bestehende Maßnahmen
	• Die Daten, die Nutzer*innen des digitalen Identitätsnachweises einem *Dritten*, der ebenfalls die entsprechende Applikation nutzt, aus der Gesamtheit der im IDR/ZMR/ERnP gespeicherten Daten zur Verfügung stellen können, sind durch den Verantwortlichen unter Beachtung des Gebots zur Datenminimierung festgelegt worden. • Aktuell besteht die Möglichkeit, die Altersstufe mithilfe der Funktion „Altersnachweis“ zu übermitteln.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen) Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Eingeschränkt (2)	Gering (1) Kommentar: Bei der Nutzung des digitalen Nachweises der Identität als Altersnachweis werden (etwa im Vergleich zum digitalen Führerschein) außerhalb der Identitätsdaten keine weiteren Daten (zB Meldeadresse) übermittelt.	Vernachlässigbar (2)

5.2.17 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.[184] • Das System wird über die Website oesterreich.gv.at via FAQs zu Sicherheit und Datenschutz grundlegend erklärt. • Es wird eine Datenschutz-Folgenabschätzung durchgeführt und der Bericht darüber wird der Öffentlichkeit zur Verfügung gestellt.

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

[184] Die Datenschutzerklärung kann in der entsprechenden Applikation abgerufen werden.

5.2.18 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 Identitätsdaten 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.[185] 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 für weite Teile der Bevölkerung möglichst einfach verfügbar zu machen bzw die Nutzung zu fördern. • Verarbeitung entgegen den Datenschutzgrundsätzen (Art 5 DSGVO) durch die Verflechtung einer staatlichen E-Government-Anwendung mit

[185] Gerichtshof der Europäischen Union PRESSEMITTEILUNG Nr. 91/20 Luxemburg, den 16. Juli 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf (abgerufen am 15.05.2024)

	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.	Eingeschränkt (2) Kommentar: Gilt, solange das Trans-Atlantic Data Privacy Framework in Kraft ist. Ansonsten gilt die Stufe Wesentlich (3).	Normal (8)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Physische Ausweise können weiterhin diskriminierungsfrei in allen Lebenslagen verwendet werden. • Verwaltungsprozesse stehen den Betroffenen nach wie vor auch „analog“ ohne Smartphone zu Verfügung. • Daten, die für die Funktionen der App benötigt werden, werden nur im lokalen App-Speicher verwendet und nicht zu iCloud oder äquivalenten Systemen übertragen.

4) Risikoanalyse und Bewertung nach (bestehenden bzw zusätzlichen Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3) Kommentar: Wie in den angeführten Maßnahmen ersichtlich, bestehen Alternativen.	Eingeschränkt (2) Kommentar: Gilt, solange das Trans-Atlantic Data Privacy Framework in Kraft ist. Ansonsten gilt die Stufe Wesentlich (3).	Normal (6)

5.3 Diskussion der verbleibenden Risiken und Folgenabschätzung

Die vorliegende Analyse zeigt, dass – nach Ermittlung und Zuordnung der bestehenden technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen – 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.[186]

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.[187]

Ebenfalls gilt es – neben den hier geprüften und analysierten Risiken – gesamtgesellschaftliche Entwicklungen zu berücksichtigen.

So sind allfällige Tendenzen eines potenziellen gesellschaftlichen Ausschlusses oder einer möglichen Ungleichbehandlung als Folge des Technologieeinsatzes kritisch zu beobachten und durch entsprechende Maßnahmen zu adressieren. Dabei geht es insb um Konsequenzen für jene Personen bzw Bevölkerungsgruppen, welche digitale Ausweise oder Nachweise aus verschiedenen Gründen nicht verwenden möchten oder können.

[186] Siehe Art 5 Abs 2 sowie Art 35 Abs 11 DSGVO.
[187] Siehe ErwGr 84 DSGVO; vgl *Martin* et al, Datenschutz-Folgenabschätzung 49.

6 Fazit und getroffene Entscheidungen

Im Ergebnis zeigt die vorliegende DSFA, dass die identifizierten verbleibenden Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der gesetzten Maßnahmen des *Verantwortlichen* nicht als hoch einzustufen sind. Aus derzeitiger Sicht besteht somit auch kein Erfordernis zur Konsultation der Aufsichtsbehörde gem Art 36 DSGVO. Die Notwendigkeit und Verhältnismäßigkeit der untersuchten Datenverarbeitungsprozesse werden auf Basis der entsprechenden systematischen Analyse in Verbindung mit den Rechtsgrundlagen und unter Berücksichtigung aller technischen und organisatorischen Maßnahmen als gegeben erachtet.

6.1 Zusammenfassung der Ergebnisse

Zusammenfassend kann festgehalten werden, dass

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

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

6.2 Pflicht zur künftigen Überprüfung

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

Eine derartige Neubewertung kann sich insb durch Änderungen am gegenständlichen System, durch technische Entwicklungen aber auch durch normative Änderungen der einschlägigen Rechtsvorschriften oder durch Gerichtsentscheidungen ergeben und im Ergebnis dazu führen, dass andere oder zusätzliche Abhilfemaßnahmen für eine datenschutzkonforme Verarbeitung vorzunehmen sind.[188]

[188] 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)[189]
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
BKA:	Bundeskanzleramt
BlgNR:	Beilagen zu den stenographischen Protokollen des Nationalrates[190]
BMDW:	Bundesminister für Digitalisierung und Wirtschaftsstandort

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

BMF:	Bundesminister für Finanzen und das zugewiesene Bundesministerium als dessen Hilfsapparat
BMG:	Bundesministeriengesetz 1986 BGBl I 1986/76
BMI:	Bundesminister für Inneres und das zugewiesene Bundesministerium als dessen Hilfsapparat
BMK:	Bundesministerin für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie und das zugewiesene Bundesministerium als dessen Hilfsapparat
bPK:	bereichsspezifische Personenkennzeichen; dieses dient grundsätzlich der eindeutigen Identifikation von natürlichen Personen in einem konkreten Verwaltungsverfahren[191] 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

[191] Vgl *Feik/Randl* in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht[3] (2012), 399.

bspw:	beispielsweise
B-VG:	Bundes-Verfassungsgesetz BGBl I 1930/1
bzgl:	bezüglich
bzw:	beziehungsweise
Client-Komponente:	Entweder Digitales-Amt-App, Third-Party-App oder Mobiler Web-Browser, die/der Signaturerstellungs-Requests erstellt, übermittelt und empfängt
CNIL:	französische Datenschutzbehörde
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 na-

	türlicher 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 18013-5:	ISO-Standard: Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application
iSv:	im Sinne von
iVm:	in Verbindung mit
iZm:	im Zusammenhang mit
leg cit:	legis citatae, der zitierten Norm
lit:	litera/literae
krit:	Kritisch

MDS:	Minimaldatensatz (bzw Minimal Dataset)
MSISDN:	Mobile Station Integrated Services Digital Network – weltweit eindeutige Mobilfunk-Rufnummer
mwN	mit weiteren Nachweisen
Nr:	Nummer
oÄ:	oder Ähnliches
OIDC:	Open ID Connect
Personenbindung:	Dadurch wird dem E-ID-Inhaber von der SZRB elektronisch signiert oder besiegelt bestätigt, dass ihm ein oder mehrere bereichsspezifische Personenkennzeichen zugeordnet sind. Die Personenbindung 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.[192]
PVP:	Portalverbundprotokoll; wird ua dazu verwendet, um auf das SPRS zuzugreifen
Rn:	Randnummer
Rsp:	Rechtsprechung
Rz:	Randziffer

[192] https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund. (abgerufen am 15.05.2024).

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)
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[193]
SZRB:	Stammzahlenregisterbehörde; nunmehr im Wirkungsbereich des BMF[194]
tlw:	teilweise
TOM(s):	(geeignete) technische und organisatorische Maßnahmen gem DSGVO[195]
ua:	unter anderem

[193] Vgl § 2 Z 8 E-GOVG.
[194] Siehe erläuternd https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 15.05.2024).
[195] Siehe etwa Art 24, 32 DSGVO.

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
vbPK-ZP	verschlüsseltes bereichsspezifisches Personenkennzeichen des Bereichs Personenidentität und Bürgerrechte
VDA:	*Vertrauensdiensteanbieter*; ein Dienst, der elektronische Signaturen, Siegel oder Zertifikate erstellt, überprüft und validiert sowie aufbewahrt[196]
vgl:	vergleiche
VO:	Verordnung
Z:	Ziffer
zB:	zum Beispiel
ZMR:	Zentrales Melderegister
Zsh:	Zusammenhang

[196] https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/anbieter/liste_der_vertrauensdiensteanbieter/Anbieter.de.html (abgerufen am 15.05.2024).