Digitaler Führerschein

Datenschutz-Folgenabschätzung

Research Institute – Digital Human Rights Center

Digitaler Führerschein

Datenschutz-Folgenabschätzung

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

Wien, August 2022

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

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	16.03.2022	V 0.1	Erstellung der Berichtsstruktur	Walter Hötzendorfer	Berichtsstruktur
2	01.04.2022	V 0.5	Erste Version des Sachverhalts und der Rechtsgrundlagen festgehalten	Walter Hötzendorfer	in Arbeit
3	05.04.2022	V 0.6	Überarbeitete Version des Sachverhalts, der Rechtsgrundlagen und erste Version der Rollenverteilung zum Review	Walter Hötzendorfer	in Arbeit
4	19.04.2022	V 0.6b	Feedback und Ergänzungen seitens BMDW und BRZ	Axel Honfi	Feedback
5	20.05.2022	V 0.93	Einbau letzter Erkenntnisse hinsichtlich Sachverhalt, Entwurf Risikobeurteilung	Walter Hötzendorfer	in Arbeit
6	15.06.2022	V 0.93b	Feedback und Ergänzungen seitens BMDW und BRZ	Patrick Silli	Feedback
7	08.07.2022	V 0.94	Feedback zu den Bearbeitungen und Kommentierungen seitens BMDW und BRZ in Kapitel 5	Walter Hötzendorfer	in Arbeit
8	12.07.2022	V 0.94b	Ergänzungen und Bereinigungen seitens BMDW nach gemeinsamer Diskussion der Risikoanalyse	Patrick Silli	Feedback
9	14.07.2022	V 0.95	Ergänzungen insb im Sachverhalt und betreffend Protokollierung	Walter Hötzendorfer	in Fertigstellung
10	09.08.2022	V 0.95b	Feedback und Ergänzungen seitens BMF, A-SIT und Youniqx	Patrick Silli	in Fertigstellung
11	10.08.2022	V 0.96	Management-Summary, Protokollierungskonzept, Fazit, Verbleibende Risiken, Feedback zu den Bearbeitungen und Kommentierungen	Walter Hötzendorfer	in Fertigstellung
12	16.08.2022	V 0.96b	Feedback und Ergänzungen seitens BMF	Patrick Silli	in Fertigstellung
13	17.08.2022	V 0.97	Umsetzung gemeinsam besprochener Korrekturen und Ergänzungen	Walter Hötzendorfer	in Fertigstellung
14	19.08.2022	V 0.97b	Feedback und Ergänzungen seitens BMF	Patrick Silli	in Fertigstellung
15	24.08.2022	V 1.0	Fertigstellung	Walter Hötzendorfer	final
16	12.09.2022	V 1.1	Umsetzung einiger Korrekturen	Walter Hötzendorfer	final
17	18.10.2022	V 1.2	Umsetzung einiger Korrekturen	Walter Hötzendorfer, Axel Honfi, Patrick Silli	final

Disclaimer

Sofern im Folgenden nicht anders angegeben, wurden alle Internetlinks zuletzt am 23. 8. 2022 abgerufen.

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

Inhalt

1 Management Summary

Der vorliegende Bericht dokumentiert die Ergebnisse der Datenschutz-Folgenabschätzung (DSFA) betreffend den Digitalen Führerschein. Dieses System ermöglicht es Führerscheininhaber*innen, ihren Führerschein digital mittels der App eAusweise sowohl gegenüber Privaten als auch im Zuge von Verkehrskontrollen gegenüber Exekutivorganen vorzuweisen. Führerscheininhaber*innen haben somit künftig die Wahl, ihren Führerschein wie bisher in physischer Form oder nunmehr mittels eAusweise-App in digitaler Form vorzuweisen. Die Möglichkeit, physische Ausweise zu verwenden, bleibt wie bisher unverändert und uneingeschränkt bestehen. Niemandem soll durch den Verzicht auf digitale Ausweise ein Nachteil entstehen.

Der digitale Führerschein baut auf dem ID Austria System auf. Zu ID Austria wurde gesondert eine DSFA durchgeführt und der DSFA-Bericht veröffentlicht.[1] Dieses System erweitert die bisher bekannten Nutzungsmöglichkeiten von Handy-Signatur und Bürgerkarte, sodass künftig neben dem Minimaldatensatz (MDS) bestehend aus Vor-, Nachname und Geburtsdatum auch weitere Personenmerkmale (Attribute) wie zB Führerschein- und Meldedaten verarbeitet werden können und durch die betroffene Person für bis zu drei Monate offline gespeichert und Dritten vorgewiesen werden können.

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

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

- Initiale Anmeldung an der eAusweise-App und Einrichtung;
- Führerschein laden;
- Verkehrskontrolle;
- Ausweis offline vorweisen (außer Verkehrskontrolle);
- Widerruf des Gerätezertifikats AWP;
- Abmelden von der eAusweise-App;
- Überprüfen des Ausweises in der eAusweise-App;
- eAusweis Check-App.

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

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

[1] https://www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf (abgerufen am 1. 8. 2022).

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, wobei anzumerken ist, dass entsprechend den bestehenden rechtlichen Grundlagen die in ISO/IEC 18013-5 vorgesehene Möglichkeit, dass die betroffene Person nur ausgewählte Daten des digitalen Führerscheins, wie zB das Geburtsdatum, vorweisen kann (selective disclosure), aktuell nicht umgesetzt ist;
- personenbezogene Daten einem stringenten Löschkonzept unterliegen;
- gespeicherte personenbezogene Daten strengen Zugriffsrechten unterliegen;
- der Grundsatz der Datenminimierung und das Prinzip „Privacy by Design“ insbesondere durch die Implementierung des Vorweisens des digitalen Ausweises als Vorgang, der vollständig offline, ohne die Beteiligung eines Servers stattfindet, bereits in der grundlegenden Gestaltung des Systems berücksichtigt wurden;
- die Protokollierung auf das technisch notwendige Minimum beschränkt ist und insbesondere Vorgänge des Vorweisens und Überprüfens von Ausweisen im System der Ausweisplattform nicht protokolliert werden.

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

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 Führerschein. 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 Digitalisierung und Wirtschaftsstandort* (BMDW) das *Research Institute – Digital Human Rights Center* (RI) im Februar 2022 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 BMDW hin zum beim *Bundesministerium für Finanzen* (BMF) neu eingerichteten Staatssekretariat unter der Leitung von Herrn Staatssekretär Florian Tursky, Msc. MBA. kam. Soweit wie 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[2] 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)[3] oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten[4] (gem Art 10 DSGVO) durchgeführt wird;
- oder eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche vorgenommen wird.

Darüber hinaus haben die Aufsichtsbehörden eine Liste mit Verarbeitungsvorgängen zu veröffentlichen, für die eine DSFA verpflichtend durchzuführen ist („Blacklist“), und können zudem eine Liste mit Verarbeitungsvorgängen veröffentlichen, für die eine DSFA nicht verpflichtend ist („Whitelist“).[5] Beides hat die österreichische Datenschutzbehörde getan.[6]

Nach der DSFA-AV („Whitelist“) sind Datenschutz-Folgenabschätzungen unter anderem dann nicht verpflichtend durchzuführen, wenn die Verarbeitung personenbezogener Daten[7] im Rahmen von Registern, die durch Unions-, Bundes-, oder Landesrecht eingerichtet sind, erfolgt.[8]

Demgegenüber ist eine DSFA nach der sogenannten „Blacklist“ der DSB verpflichtend durchzuführen, wenn unter anderem[9] 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

---

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

[3] 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.

[4] 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.

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

[6] 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.

[7] Mit Ausnahme von Daten iSd Art 9 und 10 DSGVO.

[8] DSFA-A06 Anlage 1 DSFA-AV.

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

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

3 Darstellung des Sachverhalts und Spezifizierung des Prüfgegenstands

Mit der Novellierung des E-Government-Gesetzes[10] 2017 kam es zu einer Weiterentwicklung von „Bürgerkarte“ bzw „Handy-Signatur“ zum „E-ID“.[11] Unter der Bezeichnung „ID Austria“ wird dieser elektronische Identitätsnachweis nunmehr zur eindeutigen Identifikation der Bürger*innen gegenüber digitalen Anwendungen und Diensten sowohl aus dem behördlichen als auch privaten Umfeld eingeführt. Durch den E-ID soll es Bürger*innen möglich sein, sich online auszuweisen, digitale Services zu nutzen und Geschäfte rechtsverbindlich auf elektronischem Wege abzuschließen.

Dabei wurden die bisher bekannten Nutzungsmöglichkeiten von Handy-Signatur und Bürgerkarte mit Einführung der ID Austria erweitert, sodass künftig neben dem Minimaldatensatz (MDS) bestehend aus Vor-, Nachname und Geburtsdatum auch weitere Personenmerkmale (Attribute) wie zB Führerschein- und Meldedaten verarbeitet werden können.[12]

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

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

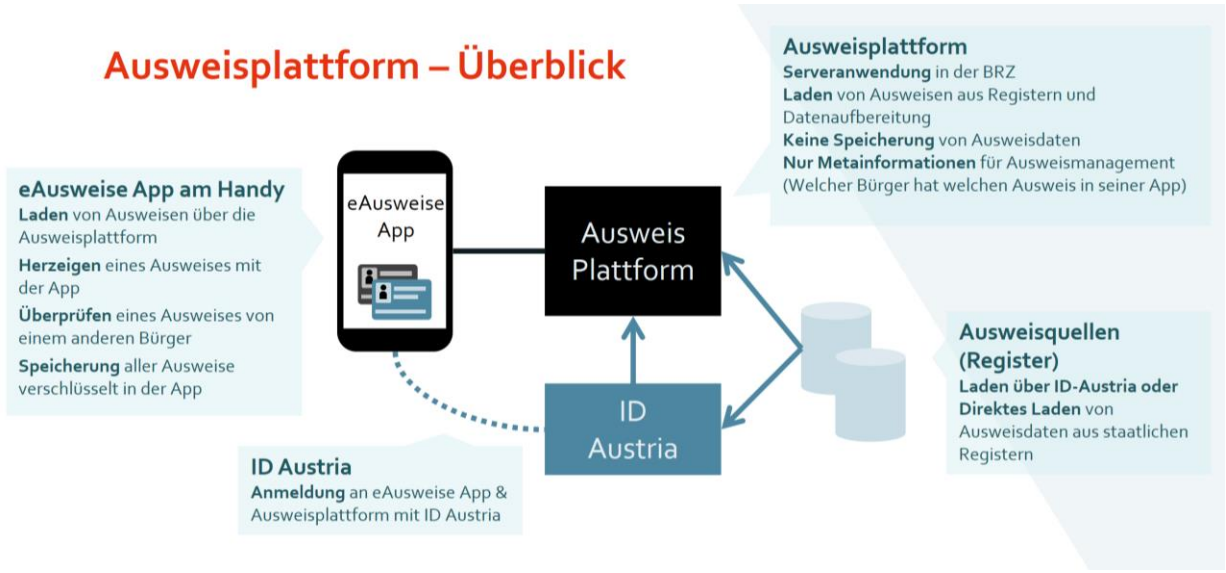

Abbildung 1: Überblick über die Systemteile

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

Ausweisplattform

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

Digitaler Ausweis

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

eAusweise-App

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

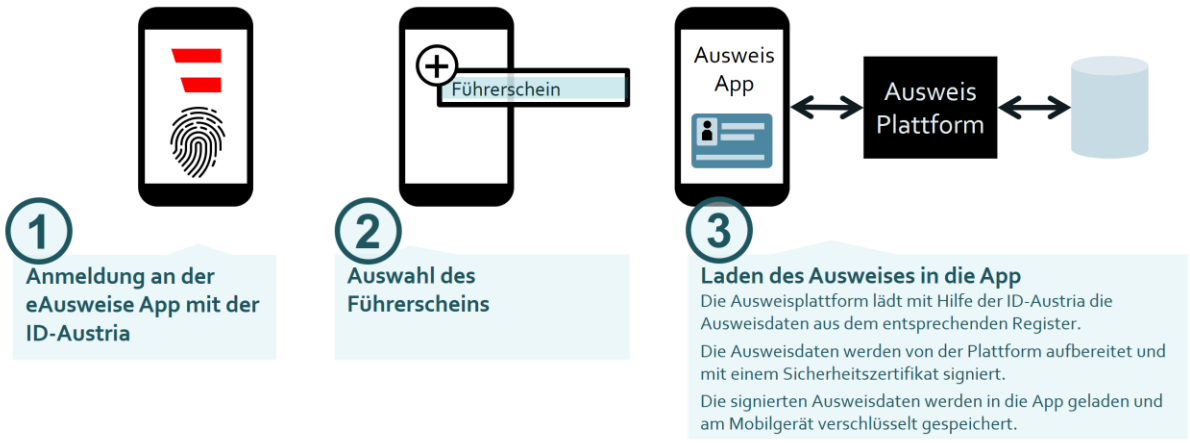

Abbildung 2: Überblick über die Funktionsweise eAusweise-App/Ausweisplattform

Durch das vorgesehene Konzept ist gewährleistet, dass die entsprechenden Ausweisdaten aus dem entsprechenden Register nur verschlüsselt in der eAusweise-App der Nutzer*innen gespeichert werden, nicht jedoch auch in der Ausweisplattform. In der Ausweisplattform werden nur Metainformationen (wie etwa welcher Ausweis von welche*r Nutzer*in geladen wurde) gespeichert.

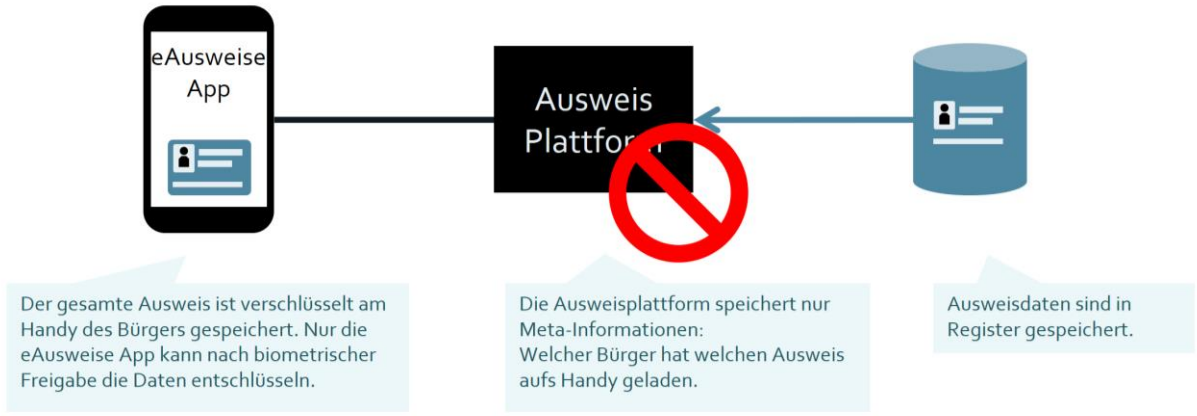

Abbildung 3: Überblick über die Speicherorte von Daten

Die eAusweise-App bietet auch die Funktionalität zum Überprüfen von Ausweisen, die eine andere Person mit ihrer eAusweise-App vorzeigt.

Die App ist (kostenlos) via Download über den „Play Store“ von Google sowie den „App Store“ von Apple erhältlich.

Die eAusweise-App ist ein Angebot, das Bürger*innen optional anstelle von physischen Ausweisen verwenden können. Es besteht für niemanden eine Pflicht oder ein faktischer Zwang, die eAusweise-App anstelle eines physischen Ausweises zu verwenden. Die Verwendbarkeit von physischen Ausweisen erfährt durch die eAusweise-App keinerlei Einschränkungen.

Anonyme Überprüfungs-App (eAusweis Check-App)

Um zum Überprüfen von Ausweisen nicht zwingend die eAusweise-App verwenden zu müssen, die eine Authentifizierung der Nutzer*innen voraussetzt, gibt es zusätzlich eine eigenständige Überprüfungs-App deren Nutzung keiner Authentifizierung der Nutzer*innen bedarf. Einziger Zweck dieser App ist die Überprüfung von Ausweisen, die eine andere Person mit ihrer eAusweise-App vorzeigt.

Auch diese App ist (kostenlos) via Download über den „Play Store“ von Google sowie den „App Store“ von Apple erhältlich.

Gemeindewachkörper-App (GWK Check-App)

Die GWK Check-App ermöglicht Organen der Gemeindewachkörper[13], Einsicht in die Führerscheindaten im Führerscheinregister zu nehmen sowie gegebenenfalls Eintragungen im Zusammenhang mit der vorläufigen Abnahme eines Führerscheins vorzunehmen, wenn eine kontrollierte Person im Rahmen einer Verkehrskontrolle die eAusweise-App vorweist (siehe hierzu im Detail bei der Verarbeitungstä-

[13] Wachkörper sind gem Art 78d Abs 1 B-VG *“[...] bewaffnete oder uniformierte oder sonst nach militärischem Muster eingerichtete Formationen, denen Aufgaben polizeilichen Charakters übertragen sind.”;* Gemeinden können solche Wachkörper, die als Hilfsorgane der Gemeindebehörden tätig werden, errichten, um Gemeindeaufgaben mit polizeilichem Charakter zu besorgen (*Grabenwarter/Frank*, B-VG Art 118 Rz 15 mit Verweis auf VfSlg 3108/1956 [Stand 20. 6. 2020, rdb.at]). Siehe zur Problematik der Abgrenzung der Begrifflichkeiten *“Gemeindewachen”* bzw *“Gemeindewachkörper”* sowie des § 35 FSG (Bundesgesetz über den Führerschein [Führerscheingesetz - FSG] BGBl I 1997/12) im Hinblick auf den verfassungsrechtlich zulässigen Einsatz von Gemeindewachkörpern als Exekutivorgane darüber hinaus: *Triendl*, Angehörige von Gemeindewachkörpern als Organe der Straßenaufsicht, ZVR 2007/2 (4 f bzw 7 mwN).

tigkeit Verkehrskontrolle). Das Erfordernis des Bestehens der „GWK Check-App“ als eigenständige Applikation ergibt sich aus dem Umstand, dass auch Organe der Gemeindewachkörper zur Durchführung von Führerschein- und Verkehrskontrollen im Allgemeinen berufen sind,[14] diese Organe jedoch nicht dem BMI unterstellt sind.

Der Zugriff auf das Führerscheinregister unter Verwendung der GWK Check-App ist ausschließlich den genannten Organen der Gemeindewachkörper nach Authentifizierung eines befugten Organs möglich (siehe dazu Abschnitt 3.2.3.2).

Der Prüfgegenstand der vorliegenden Datenschutz-Folgenabschätzung (DSFA) gliedert sich somit in folgende Systemteile:

- Ausweisplattform;
- eAusweise-App;
- eAusweis Check-App;
- GWK Check-App.

Gegenstand der vorliegenden DSFA sind daher die nachfolgend angeführten Verarbeitungstätigkeiten:

- Initiale Anmeldung an der eAusweise-App und Einrichtung;[15]
- Führerschein laden;[16]
- Verkehrskontrolle;[17]
- Ausweis offline vorweisen (außer Verkehrskontrolle);[18]
- Widerruf des Gerätezertifikats AWP;[19]
- Abmelden von der eAusweise-App;[20]
- Überprüfen des Ausweises in der eAusweise-App;[21]
- eAusweis Check-App.[22]

Gänzlich außerhalb der Verantwortlichkeit des BMF und daher nicht Gegenstand der vorliegenden DSFA sind der Betrieb des Führerscheinregisters (FSR), welches unabhängig vom digitalen Führerschein besteht und vom Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK) geführt wird, sowie die Verarbeitung personenbezogener Daten durch jene Personen, denen die betroffene Person den digitalen Führerschein vorweist, einerseits im Fall eines Organs der Bundespolizei im Zuge einer Verkehrskontrolle, dies fällt in die datenschutzrechtliche Verantwortlichkeit des Bundesministeriums für Inneres (BMI) bzw der Landespolizeidirektionen (LPD), und andererseits im Fall des Vorweisens gegenüber Privaten, dies fällt in deren jeweilige datenschutzrechtliche Verantwortlichkeit. Wie erwähnt sehr wohl Gegenstand der vorliegenden DSFA ist die - durch das BMF 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.

[14] Vgl § 14 Abs 1 iVm § 35 Abs 2 und 3 FSG.
[15] Siehe dazu im Detail 3.2.1.
[16] Siehe dazu im Detail 3.2.2.
[17] Siehe dazu im Detail 3.2.3.
[18] Siehe dazu im Detail 3.2.4.
[19] Siehe dazu im Detail 3.2.5.
[20] Siehe dazu im Detail 3.2.6.
[21] Siehe dazu im Detail 3.2.7.
[22] Siehe dazu im Detail 3.2.8.

3.1 Technische Architektur

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

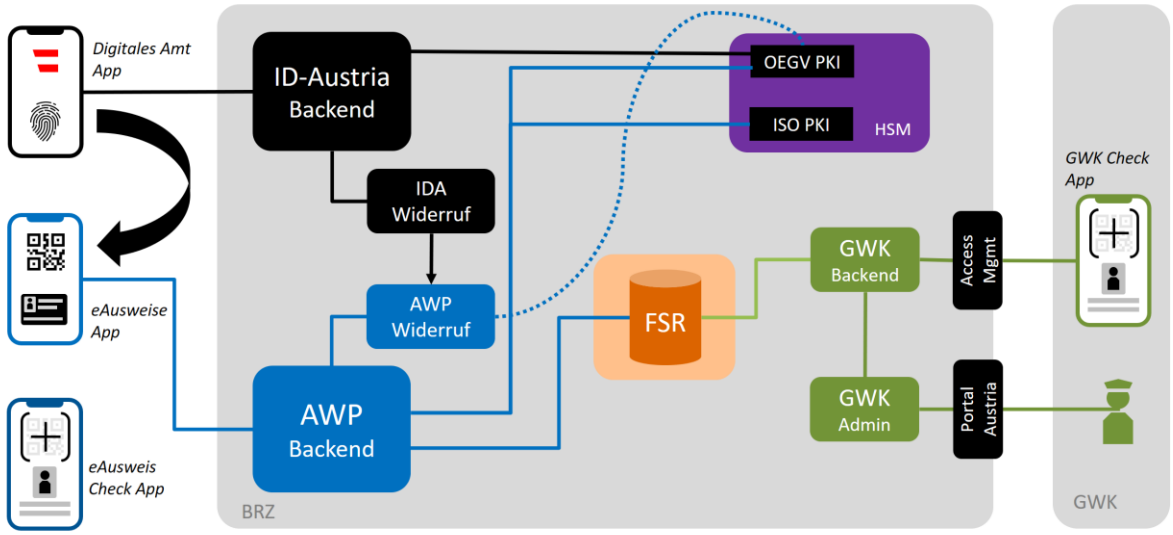

Abbildung 4: Architektur des Systems und Schnittstellen zwischen den einzelnen Komponenten

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 authentisieren und erforderlichenfalls in eine Datenübermittlung einwilligen.

IDA/DA Backend

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

Ausweis App

Die eAusweise-App ist Frontend und User Interface für den Bürger für die Ausweisplattform.

Ausweisplattform (AWP) Backend

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

eAusweis Check-App

Die eAusweis Check-App ermöglicht die einfache Überprüfung von Ausweisen, ohne eine Anmeldung der Nutzer*innen vorauszusetzen.

ID Austria Widerrufsservice

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

AWP Widerrufsservice

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

HSM - Hardware Security Module

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

FSR - Führerscheinregister

Im Führerscheinregister (FSR) sind alle österreichischen Führerscheine historisch gespeichert. Es wird im Bundesrechenzentrum betrieben und exponiert zwei Schnittstellen:

a) die IAP-Schnittstelle für Zugriffe durch die Exekutive sowie

b) eine REST-Schnittstelle für das Laden von Führerscheindaten durch den betroffenen Bürger selbst über die Ausweisplattform.

Die IAP-Schnittstelle ist von außerhalb des Bundesrechenzentrums über das Portalverbundprotokoll aufrufbar.

GWK Check-App und Backend

Die Gemeindewachkörper bekommen für die Durchführung von Verkehrskontrollen die GWK Check-App zur Verfügung gestellt. Diese App kann über ein eigenes Backend im Bundesrechenzentrum Führerscheindaten laden und anzeigen.

GWK Check-Admin und Portal Austria

Für die Verwaltung der Beamt*innen der Gemeindewachkörper im Zusammenhang mit der GWK Check-App steht im Portal Austria eine eigene Administrations-Anwendung zur Verfügung. Das Portal Austria ist ein zentrales Access Management Portal im Bundesrechenzentrum für den sicheren Zugang zu Webanwendungen der Verwaltung.

3.2 Die einzelnen Datenverarbeitungstätigkeiten

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

3.2.1 Initiale Anmeldung an der eAusweise-App und Einrichtung

Zweck dieser Verarbeitungstätigkeit ist die Einrichtung der eAusweise-App auf dem Endgerät der Nutzer*in, sodass sie dieser für die Verwendung zur Verfügung steht. Dies kann auch durch den Ablauf der Gültigkeit der gespeicherten Daten nach 90 Tagen oder jener des Gerätezertifikats nach neun Monaten erforderlich werden. Die Nutzer*in installiert zunächst die eAusweise-App. Zur initialen Anmeldung startet die Nutzer*in zunächst die eAusweise-App und klickt auf den Button “Anmelden über Digitales-Amt”. Voraussetzung für die Anmeldung in der eAusweise-App ist, dass auf demselben Endgerät auch die Digitales-Amt-App installiert ist. Ist dies nicht der Fall, wird die Nutzer*in bei der Anmeldung zur Installation der Digitales-Amt-App aufgefordert. Ist diese installiert, wird die Nutzer*in in die App “Digitales Amt” weitergeleitet, führt dort die Anmeldung über die ID Austria durch und willigt erforderlichenfalls in die Übermittlung ihrer personenbezogenen Daten zur eAusweise-App ein. Im Anschluss wird diese*r wieder in die eAusweise-App zurückgeleitet.

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

Die Nutzer*in befindet sich dabei zunächst in der eAusweise-App, die sich **am selben** Gerät wie die Digitales-Amt-App befindet. Die eAusweise-App agiert im Rahmen der ID Austria als Service Provider (SP). Die eAusweise-App erstellt einen Authentifizierungs-Request (also eine Anfrage), der an die Digitales-Amt-App und von dort weiter an den Identity Provider der ID Austria (IDP) übermittelt wird. Nach erfolgter Authentifizierung stellt der IDP einen Registrierungstoken aus und übermittelt diesen an die eAusweise-App und die Nutzer*in wird in die eAusweise-App geleitet. Die Ausweisplattform nimmt den Registrierungstoken entgegen, validiert diesen über die ID Austria und erstellt für die Nutzer*in daraufhin ein entsprechendes App-Zertifikat. Daraufhin wird der Registrierungstoken in der Ausweisplattform gelöscht.

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

Folgende Daten werden dabei verarbeitet:

- Minimal Data Set (MDS)
- bPK des Bereichs ZP-MH (als Primärschlüssel)
- verschlüsseltes bPK des Bereichs Verkehr und Technik[23] (vbPK-VT), um den Führerschein laden zu können

[23] Die Verschlüsselung erfolgt so, dass die Entschlüsselung nur beim Zugriff auf das Führerscheinregister möglich ist; siehe zum bPK-VT auch: Teil 1 der Anlage zu § 3 Abs 1 E-Government-Bereichsabgrenzungsverordnung BGBl II 2004/289.

- Signaturzertifikat der Nutzer*in[24]
- ID Austria Full oder Basic User[25]
- Mitgliedstaat der Nutzer*in[26]
- IP-Adresse des Endgeräts der Nutzer*in[27]
- Registrierungstoken (ID-Token)

MDS, bPK-ZP-MH, vbPK-VT, Mitgliedstaat der Nutzer*in, Signaturzertifikat und die Information, ob eine ID Austria Full vorliegt, werden serverseitig in der Ausweisplattform in einer verschlüsselten Datenbank gespeichert, in der eAusweise-App der Nutzer*in lediglich der MDS und das vbPK-VT.[28]
Zur initialen Einrichtung der eAusweise-App muss die Nutzer*in zunächst den Nutzungsbedingungen zustimmen und bestätigen, dass er*sie die Datenschutzinformation zur Kenntnis genommen hat. Um sich in Zukunft ausschließlich über die eAusweise-App anmelden zu können, muss sich die Nutzer*in biometrisch authentisieren, um diese Login-Methode für die App einzurichten. Ist dies erfolgt, kann die App künftig über eine biometrische Authentisierung ohne Sprung zur Digitales Amt App gestartet werden. Erfolgt dies nicht, kann die eAusweise-App nicht verwendet werden. Mit anderen Worten, ohne Verwendung der biometrischen Authentisierung kann die eAusweise-App nicht verwendet werden.

Meldet sich die jeweilige Nutzer*in von der eAusweise-App ab, werden in der App alle personenbezogenen Daten der Nutzer*in gelöscht und die initiale Anmeldung muss ggf erneut durchgeführt werden. Die Abmeldung von der eAusweise-App (“dieses Gerät abmelden“) wird zudem an die Ausweisplattform kommuniziert und führt serverseitig jedenfalls zur Löschung der Daten in Bezug auf das verwendete Gerät, und falls dieses das einzige Gerät ist, auf dem die Nutzer*in die eAusweise-App eingerichtet hat, zur Löschung aller serverseitig gespeicherten personenbezogenen Daten.

3.2.2 Führerschein laden

Zweck dieser Verarbeitungstätigkeit ist es, den digitalen Führerschein auf das Endgerät der Nutzer*in zu laden. Das ist erforderlich, um den digitalen Führerschein verwenden zu können, und somit eine Voraussetzung für die nachfolgend beschriebenen Verarbeitungstätigkeiten. Dazu wählt die Nutzer*in in der eAusweise-App die entsprechende Funktion zum Herunterladen des Führerscheins auf das eigene Endgerät aus. Die eAusweise-App authentifiziert sich dabei mit dem entsprechenden Gerätezertifikat an der Ausweisplattform. Mittels des entsprechenden vbPK-VT lädt die Ausweisplattform die Führerscheindaten aus dem Führerscheinregister, bereitet diese Daten auf und übermittelt diese signiert an die eAusweise-App.[29]

[24] Als Ergebnis der Datenverarbeitung bei der Anmeldung mittels ID Austria stellt die Ausweisplattform der eAusweise-App ein App-Zertifikat aus. Dieses enthält Name und Vorname der Nutzer*in, wird anschließend biometrisch gesichert im Ausweisplattform-Backend gespeichert und in Zukunft für die Authentisierung am Backend verwendet, wobei die Gültigkeit der jeweiligen ID Austria überprüft wird.
[25] Nur bei Vorliegen eines ID Austria Full User, nicht also, wenn ein erleichterter Umstieg von der Handy-Signatur erfolgt ist (= Basic User), ist eine Nutzung der eAusweise-App möglich.
[26] Dies ist deswegen notwendig, weil nur bei Österreicher*innen ein entsprechendes Signaturzertifikat vorhanden ist.
[27] Diese wird sowohl an das ID Austria System als auch an die Ausweisplattform übermittelt.
[28] Dies erfolgt unter Anwendung einer AES-256-Verschlüsselung im Filesystem der Ausweisapp, wobei der Schlüssel je nach Betriebssystem bzw Hersteller des Endgeräts im Secure Element des Gerätes (Android Keystore bzw in der Secure Enclave (Apple)) gespeichert wird.
[29] Die Signaturlaufzeit wird dabei an die Zertifikatslaufzeit der jeweiligen ID Austria angepasst.

Die Führerscheindaten werden ausschließlich im Filesystem der eAusweise-App am mobilen Endgerät (mittels AES-256-Algorithmus) verschlüsselt gespeichert, nicht jedoch serverseitig.

Für das Laden des Führerscheins ist die Inhaberschaft eines Führerscheins im Scheckkartenformat zwingende Voraussetzung. Nur dann ist ein entsprechendes Lichtbild im Führerscheinregister gespeichert, welches geladen werden kann. Dies hat den Hintergrund, dass lediglich auf das Führerscheinregister (FSR) zugegriffen wird, nicht jedoch auch auf das Identitätsdokumentenregister oÄ.

In der Folge werden in der eAusweise-App die Anwendungsfälle “Verkehrskontrolle” und “Führerschein” verfügbar (siehe zu beidem sogleich).

Folgende Daten werden hierbei verarbeitet:

- Berechtigungs-ID (dient zur Verknüpfung von Person und Ausweis im Backend)
- vbPK-VT
- Familienname
- Vorname(n)
- Geburtsdatum und Geburtsort
- akademische Grade
- die Ausstellungsbehörde
- Klasse, Berechtigung oder Gruppe, für die der Führerschein ausgestellt wurde
- das Datum der erstmaligen Erteilung der Lenkberechtigung, im Fall der Wiedererteilung auch dieses Datum,
- das Datum der Ausstellung des Führerscheines
- die Führerscheinnummer
- das Lichtbild und die Unterschrift des *Antragstellers* in gescannter Form,
- allfällige Befristungen, Beschränkungen oder Auflagen und der Grund dafür

3.2.3 Verkehrskontrolle

Zweck dieser Verarbeitungstätigkeit ist das Vorweisen und Überprüfen des digitalen Führerscheins im Zuge einer Verkehrskontrolle, wenn die Nutzer*in dies gegenüber dem Vorweisen des physischen Führerscheins bevorzugt.

Im Fall der Verkehrskontrolle erfolgt die Überprüfung der Ausweisdaten, anders als in allen anderen Fällen der Verwendung des digitalen Führerscheins, durch Abruf dieser Daten aus dem Führerscheinregister (FSR) durch das befugte Organ, das die Verkehrskontrolle durchführt. Für diesen Zweck wird durch Vorweisen der eAusweise-App durch die Nutzer*in dem Endgerät des Organs mitgeteilt, von welcher Person Daten aus dem FSR abgerufen werden müssen.

3.2.3.1 Vorweisen durch die Nutzer*in

Die Nutzer*in öffnet die eAusweise-App, führt eine biometrische Authentisierung durch (siehe 3.2.1) und wählt in der eAusweise-App den Anwendungsfall “Verkehrskontrolle”. Mit der biometrischen Authentisierung wird der Schlüssel zum Signieren der vorzuweisenden Daten freigegeben. Diese Daten (siehe im Detail unten) werden daraufhin in Form eines QR-Codes angezeigt. Der QR-Code kann da-

raufhin dem Organ des öffentlichen Sicherheitsdienstes oder der Straßenaufsicht (insbesondere Bundespolizei oder Gemeindewachkörper[30]) im Rahmen der Führerscheinkontrolle vorgewiesen werden, um diesem den Abruf der Führerscheindaten der Nutzer*in aus dem Führerscheinregister zu ermöglichen, wie in der folgenden Abbildung schematisch dargestellt:

Abbildung 5: Schematische Darstellung der Ansicht zum Vorweisen des QR-Codes

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 (siehe dazu unten Abschnitt 3.2.5) die Signatur. Über das im QR-Code enthaltene vbPK-VT wird dem Organ ermöglicht, die Führerscheindaten der betroffenen Person aus dem Führerscheinregister auf sein Endgerät zu laden (siehe dazu nächster Abschnitt).

Abbildung 6: Ablauf der Überprüfung des digitalen Führerscheins bei einer Verkehrskontrolle

[30] Siehe zur Problematik der Abgrenzung der Begrifflichkeiten *"Gemeindewachen"* bzw *"Gemeindewachkörper"* sowie des § 35 FSG im Hinblick auf den verfassungsrechtlich zulässigen Einsatz von Gemeindewachkörpern als Exekutivorgane erneut *Triendl*, ZVR 2007/2 (4 f bzw 7 mwN); vgl ansonsten insb §§ 15a, 35 und 39 FSG sowie § 97 StVO.

Neben dem vbPK-VT enthält dieser QR-Code auch einen (signierten) Timestamp, wodurch eine Wiederverwendung des QR-Codes verhindert werden soll.[31]

Darüber hinaus enthält der QR-Code auch den MDS (Vorname, Nachname, Geburtsdatum). Dieser wäre zum Zweck des Abrufs der Ausweisdaten im FSR 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[32] und zum anderen, dem Organ im Falle einer mangelnden Internetverbindung Vorname, Nachname und Geburtsdatum der Person, die sich soeben im Zuge der Verkehrskontrolle mit dem digitalen Führerschein ausweist, wie beim Vorweisen eines physischen Ausweises unmittelbar ersichtlich zu machen.

Zudem sind die im QR-Code enthaltenen Daten mit einer Signatur versehen.

Folgende Daten werden somit in diesem Schritt wie beschrieben verarbeitet:

- vbPK-VT
- MDS
- Timestamp
- Signatur dieser Daten

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

[31] Denn gem § 15a Abs 1 FSG ist dies nur *Inhabern* eines E-ID, die die eAusweise-App verwenden (und über einen Scheckkartenführerschein verfügen), möglich. Die Zeitspanne bis zur Kontrolle darf dabei bis zu 15 Minuten betragen; siehe zur aufrechten E-ID-Inhaberschaft insbesondere auch 3.2.5.

[32] Im Einzelfall kann sich insbesondere der Nachname nach Ausstellung des Führerscheins geändert haben. Diese Änderung wäre nicht zwingend im FSR ersichtlich, jedoch im ZMR, aus welchem der MDS in der eAusweise-App letztlich im Wege der ID Austria stammt.

3.2.3.2 Einsichtnahme in das Führerscheinregister 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 das Führerscheinregister stets erforderlich ist, erfolgt durch eine Anmeldung mittels ID Austria, und zwar mit der persönlichen Identität des jeweiligen Gemeindewacheorgans. Es handelt sich daher um denselben Vorgang, der bereits in Kapitel 3.2.1 in Bezug auf die Nutzer*innen der eAusweise-App 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 Gemeindewacheorgans mittels eines Web-Tokens im OIDC-Standard (siehe oben Abschnitt 3.2.1) 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 Gemeindewacheorgans zu laden. Sofern dies erfolgreich ist, bleibt das Gemeindewacheorgan 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 Gemeindewacheorgan immer wieder neu durchgeführt werden.

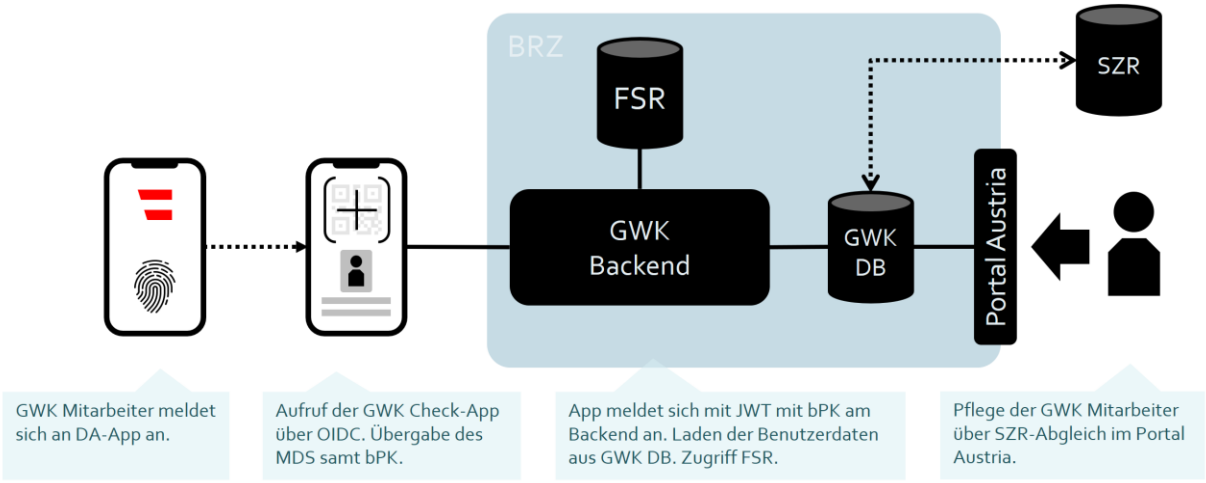

Abbildung 7: Überblick über GWK Check-App und GWK-Backend

Die Administration der jeweiligen Gemeindewacheorgane für die Zwecke dieser Applikation erfolgt in einer eigenen Admin-App über das Portal Austria[33]. Diese Administration wird von den Gemeindewachkörpern selbst durchgeführt. Dabei werden die jeweiligen Gemeindewacheorgane 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 Verkehrskontrolle verwendet werden. Wie oben ausgeführt, ermöglicht das im QR-Code enthaltene vbPK-VT der jeweiligen Nutzer*in der eAusweise-App dem bei der Verkehrskontrolle tätigen Organ, die entsprechenden Daten dieser Nutzer*in aus dem FSR auf das

[33] Siehe hierzu unter 3.1.

dienstliche Endgerät zu laden.[34] Darüber hinaus ist, wie erwähnt, auch der MDS im abfotografierten QR-Code enthalten sowie ein Timestamp und die App-Signatur, womit auf dem dienstlichen Endgerät zunächst über die Prüfung dieser Signatur bzw der damit signierten Daten unter Einbeziehung der Widerrufsliste (siehe Abschnitt 3.2.5) überprüft wird, ob der QR-Code aktuell ist.[35] Dies ist erforderlich, weil in § 15a Abs 1 FSG festgelegt ist, dass die Verwendung des digitalen Führerscheins nur bei aufrechter ID Austria und nur mittels eAusweise-App erfolgen soll. Das Vorzeigen eines Screenshots oder gar eines Ausdrucks des QR-Codes, was ansonsten im Anwendungsfall Verkehrskontrolle technisch möglich wäre, wird auf diese Weise ausgeschlossen, um den genannten gesetzlichen Anforderungen zu genügen.

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

Neben der in diesem Kapitel bereits beschriebenen Funktion des QR-Code-Scans und anschließender Abfrage bzw Anzeige der entsprechenden Daten aus dem FSR, verfügt die GWK Check-App noch über folgende Funktionen:

- Abfrage und Anzeige der entsprechenden Daten aus dem FSR über Eingabe von Vorname, Nachname und Geburtsdatum (anstatt über entsprechenden QR-Code)
- Eintragung einer vorläufigen Abnahme des Führerscheins im FSR
- Aufhebung einer vorläufigen Abnahme des Führerscheins im FSR

3.2.4 Ausweis offline vorweisen (außer Verkehrskontrolle)

Zweck dieser Verarbeitungstätigkeit ist das Vorweisen und Überprüfen des digitalen Führerscheins in allen anderen Fällen außer einer Verkehrskontrolle, wenn die Nutzer*in ihre Lenkberechtigung oder ihre Identität mit dem digitalen Führerschein nachweisen möchte.

Hierzu öffnet die Nutzer*in die eAusweise-App, führt eine biometrische Authentisierung durch (siehe Abschnitt 3.2.1) und wählt in der eAusweise-App den Anwendungsfall “Führerschein” aus. Daraufhin werden der Nutzer*in die entsprechenden Führerscheindaten angezeigt, sowie die Hinweise “Kann nicht zum Nachweis der Lenkberechtigung verwendet werden” und “Für den Nachweis der Lenkberechtigung ist eine Aktualisierung notwendig”.

[34] Im Rahmen des Anwendungsfalles “Verkehrskontrolle” ist daher weder eine Aktualisierung des vbPK-VT erforderlich (denn dieses ändert sich nicht) noch eine Aktualisierung der Führerscheindaten auf dem Mobilgerät der Nutzer*innen, denn das jeweilige Organ nimmt dabei selbst Einsicht in das FSR.

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

Abbildung 8: Schematische Darstellung der Anzeige der Führerscheindaten

Für den Nachweis der Lenkberechtigung müssen Nutzer*innen zunächst "Aktualisieren" auswählen, woraufhin die Führerscheindaten erneut aus dem FSR geladen werden und dann für bis zu 30 Minuten als Nachweis der Lenkberechtigung verwendet werden können. Hintergrund dieser Einschränkung ist, dass - zumindest 30 Minuten - vor dem Nachweis der Lenkberechtigung stets eine Überprüfung im FSR erfolgen muss, ob diese aktuell noch aufrecht ist. Diese Kontaktaufnahme mit dem FSR erfolgt auf dem Endgerät der betroffenen Person durch die betroffene Person selbst und nicht auf dem Endgerät der überprüfenden Person, damit die Überprüfung tatsächlich in jedem Fall offline stattfindet, was nicht zuletzt der Datenminimierung dient.

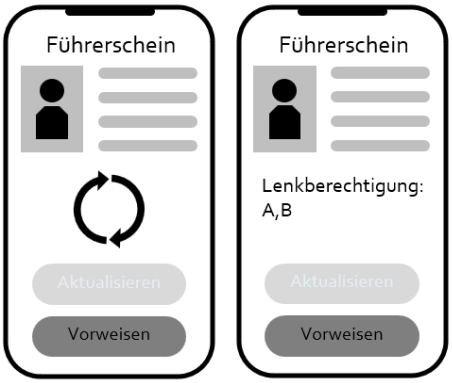

Abbildung 9: Schematische Darstellung der Aktualisierung und der Anzeige der aktualisierten Führerscheindaten

Zwar sind die Führerscheindaten auch nach Ablauf dieser 30 Minuten weiterhin am Gerät gespeichert, es wird jedoch wieder der oben erwähnte Hinweistext angezeigt. Der Ausweis kann ohne Aktualisierung jedenfalls stets für andere Zwecke als zum Nachweis der Lenkberechtigung verwendet werden. Eine Online-Aktualisierung der Daten ist zwar auch vor einer entsprechenden Überprüfung (abseits des Lenkberechtigungsnachweises) möglich, jedoch innerhalb der vorgesehenen dreimonatigen Frist nicht zwingend notwendig.[36] Nach Ablauf dieser Frist ist eine Aktualisierung der Führerscheindaten über eine neuerliche Anmeldung mittels ID Austria notwendig.

[36] Dies hat den Hintergrund, dass es sich dabei nach § 15a Abs 4 FSG um eine Form des vereinfachten Nachweises und einer entsprechenden Speicherung zum E-ID gem § 4 Abs 6 E-GovG handelt.

Um den Führerschein zur Überprüfung vorzeigen zu können, müssen Nutzer*innen zunächst in der eAusweise-App “Vorweisen” auswählen, woraufhin ein QR-Code mit einem Einmal-Token bzw Device Engagement Code (DEC) angezeigt wird. Dieser kann daraufhin zur Überprüfung vorgezeigt werden. Die Übermittlung und Überprüfung folgen dabei dem internationalen Standard ISO/IEC 18013. Der Datenaustausch besteht hierbei aus drei Phasen: Initialisierung, Device Engagement und Data Retrieval.[37]

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.[38] Darin sind Informationen darüber enthalten, welche Data-Retrieval-Methoden, dh Methoden zur Übermittlung der eigentlichen Führerscheindaten, 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.

Zur Überprüfung ruft die überprüfende Person die Überprüfungsfunktion der eAusweise-App auf ihrem Endgerät auf oder öffnet die anonyme Überprüfungs-App eAusweis Check. In beiden Fällen läuft die Überprüfung in gleicher Weise ab und beginnt mit dem Fotografieren des QR-Codes, der in der eAusweise-App der sich ausweisenden Person angezeigt wird. Daraufhin beginnt die Phase Data Retrieval. Dazu bauen die involvierten Mobilgeräte eine verschlüsselte Verbindung über Bluetooth low energy auf und es werden die Daten vom Endgerät der sich ausweisenden Person auf jenes der überprüfenden Person übertragen. Zur Verschlüsselung dieser Verbindung kommt der Standard AES-256-GCM zum Einsatz und das entsprechende Schlüsselpaar wird jeweils über HKDF gemäß RFC 5869 erzeugt.[39]

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[40] keine Internetverbindung und dieser Vorgang wird somit auch serverseitig nicht erfasst.

[37] 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).
[38] Siehe bzgl des QR-Codes insgesamt: INTERNATIONAL STANDARD ISO/IEC 18013-5 First edition 2021-09, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (8.2.2.3).
[39] 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 (9.1.1.5).
[40] 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 Lenkberechtigung erfolgen soll (siehe oben).

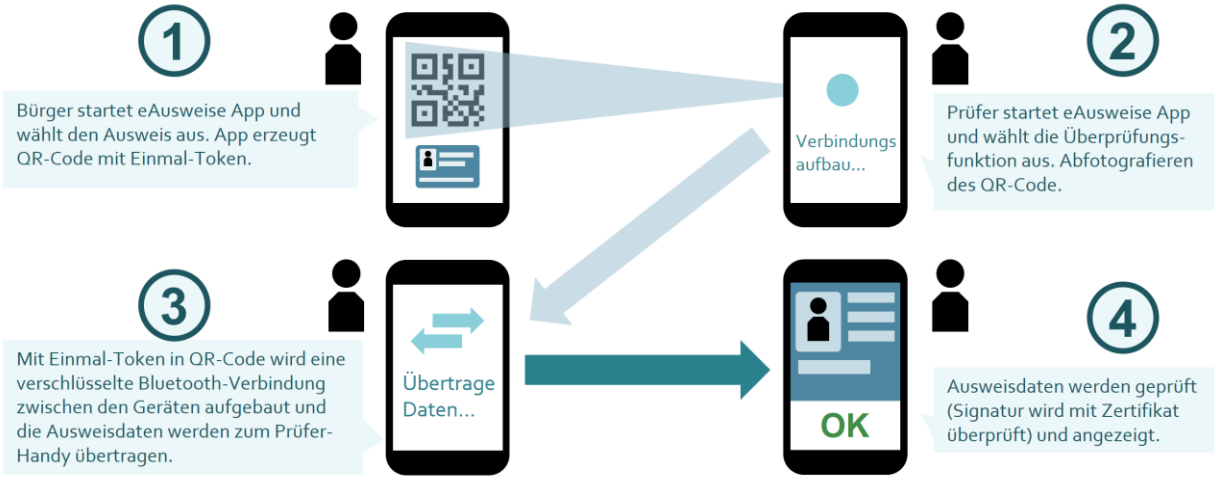

Abbildung 10: Ablauf der Ausweisüberprüfung offline, in allen anderen Fällen außer Verkehrskontrollen

Folgende Daten werden hierbei verarbeitet (in Klammern die Bezeichnungen aus dem Standard ISO/IEC 18013-5:2021):

- Familienname (family_name)
- Vorname(n) (given_name)
- Geburtsdatum (birth_date)
- Geburtsort (birth_place)
- akademische Grade (family_name[41])
- die Ausstellungsbehörde (issuing_authority)
- Klasse, Berechtigung oder Gruppe, für die der Führerschein ausgestellt wurde (driving_privileges)
- das Datum der erstmaligen Erteilung der Lenkberechtigung, im Fall der Wiedererteilung auch dieses Datum (issue_date)
- das Datum der Ausstellung des Führerscheines (issue_date[42])
- die Führerscheinnummer (document_number)
- das Lichtbild und die Unterschrift des *Antragstellers* in gescannter Form (portrait bzw signature_usual_mark)
- allfällige Befristungen (expiry_date)
- (issuing_country[43])
- (un_distinguishing_sign[44])

[41] Für akademische Grade besteht im entsprechenden ISO-Standard kein eigenes Feld; diese werden daher gemeinsam mit dem Nachnamen übertragen.
[42] Ein entsprechendes Feld wird sowohl in Bezug auf die jeweilige Lenkberechtigung als auch in Bezug auf den Führerschein in seiner Gesamtheit verwendet.
[43] Es handelt sich dabei um ein Pflichtfeld gem ISO/IEC 18013-5. Diese Angabe ist für alle österreichischen Führerscheine gleich; es handelt sich daher nicht um eine Information, die sich spezifisch auf die jeweilige betroffene Person bezieht.
[44] Es handelt sich dabei um ein Pflichtfeld gem ISO/IEC 18013-5. Diese Angabe ist für alle österreichischen Führerscheine gleich; es handelt sich daher nicht um eine Information, die sich spezifisch auf die jeweilige betroffene Person bezieht.

- (mobileSecurityObject[45])
- (errors[46])

3.2.5 Widerruf des Gerätezertifikats AWP

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

Der Widerruf des Gerätezertifikats für die Ausweisplattform erfolgt durch den Widerruf der jeweiligen ID Austria der Nutzer*in, welcher wiederum auf verschiedene Arten erfolgen kann.[47] Hierbei wird im Backend das jeweilige bPK vom ID Austria System an die Ausweisplattform übermittelt. Daraufhin wird das Gerätezertifikat der entsprechenden Nutzer*in auf eine Widerrufsliste (Certificate Revocation List, CRL) gesetzt. Diese ist implementiert als Standard-X.509v2-CRL[48] und enthält im Wesentlichen die Seriennummern der widerrufenen Zertifikate. Der Personenbezug dieser Seriennummer kann nur in der AWP sowie durch die Prüf-App im Zuge der Überprüfung des Ausweises der jeweiligen betroffenen Person hergestellt werden. Die Widerrufsliste wird beim Start der jeweiligen Prüf-App stets neu vom Server geladen und bei einem Prüfvorgang[49] mit dem Gerätezertifikat der jeweiligen Nutzer*in abgeglichen. Befindet sich das Gerätezertifikat der überprüften Person auf der Widerrufsliste, schlägt die Ausweisprüfung fehl. Kann die aktuelle Widerrufsliste beim Start der Prüf-App nicht geladen werden, insbesondere, weil keine Internetverbindung besteht, und ist die zuletzt geladene Widerrufsliste bereits älter als 48 Stunden, so kann die Ausweisprüfung zwar durchgeführt werden, es wird allerdings ein Hinweis angezeigt, dass die Widerrufsliste veraltet ist.

3.2.6 Abmelden von der eAusweise-App

Zweck dieser Verarbeitungstätigkeit ist das Löschen von Daten der Nutzer*in auf dem entsprechenden Endgerät bzw serverseitig durch die Nutzer*in selbst. Da der digitale Führerschein nach dem Herunterladen (siehe 3.2.2) lediglich in der eAusweise-App gespeichert ist, wird ein “Widerruf” des digitalen Führerscheins, wenn von der betroffenen Person gewünscht, schlicht durch das Löschen dieser Daten durch die betroffene Person in der eAusweise-App bewirkt. Hierzu wählt die Nutzer*in “Dieses Gerät abmelden” in der eAusweise-App aus. Daraufhin werden jedenfalls alle am Gerät gespeicherten Daten gelöscht. Handelt es sich beim entsprechenden Gerät um das einzige der Nutzer*in, das im Zusammenhang mit der eAusweise-App verwendet wird, werden zudem auch alle in der Datenbank serverseitig gespeicherten Daten gelöscht. Ist dies nicht der Fall, verwendet die Nutzer*in also noch auf einem Gerät die eAusweise-App, werden serverseitig lediglich die Daten in Bezug auf jenes Gerät aus der Datenbank gelöscht.[50]

---

[45] Es handelt sich dabei um ein Pflichtfeld gem ISO/IEC 18013-5.
[46] Es handelt sich dabei um ein Pflichtfeld gem ISO/IEC 18013-5.
[47] Insbesondere muss dieser nicht zwingend unmittelbar durch Nutzer*innen ausgelöst werden, sondern erfolgt etwa auch, wenn ein Rooting des Endgeräts erkannt wird.
[48] Siehe dazu https://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/X509CRL.html.
[49] Dies sowohl im Offline-Use-Case, und zwar auch beim Nachweis der Lenkberechtigung (siehe dazu jeweils 3.2.4), als auch bei der Verkehrskontrolle (siehe dazu 3.2.3).
[50] Diesfalls würden etwa Informationen darüber, welche Ausweise die Nutzer*in bezogen hat, gespeichert bleiben.

3.2.7 Überprüfen des Ausweises in der eAusweise-App

Die eAusweise-App umfasst zudem auch eine Funktion, um wie unter 3.2.4 beschrieben einen Ausweis offline zu überprüfen. Zweck dieser Verarbeitungstätigkeit ist die Verwendung dieser Funktion, um die Gültigkeit des digitalen Führerscheins einer anderen Person zu prüfen. Hierzu muss die überprüfende Person mittels ihrer ID Austria an der eAusweise-App angemeldet sein.[51] Siehe zur Anmeldung und Einrichtung sinngemäß 3.2.1. Darüber hinaus werden bei der Überprüfung selbst keine personenbezogenen Daten der überprüfenden Person verarbeitet. Zur Verarbeitung personenbezogener Daten der *zu überprüfenden* Person siehe insbesondere unter 3.2.4.

3.2.8 eAusweis Check-App

Zweck dieser Verarbeitungstätigkeit ist die Verwendung der eigenständigen und anonymen Überprüfungs-App, um die Gültigkeit des digitalen Führerscheins einer anderen Person zu prüfen. Hierbei werden keine personenbezogenen Daten der Nutzer*innen dieser Ausweis-Überprüfungs-App verarbeitet. Zur Verarbeitung personenbezogener Daten der *zu überprüfenden* Person siehe insbesondere unter 3.2.4.

[51] Zum Überprüfen von Ausweisen durch Nutzer*innen, die nicht bereits die eAusweise-App zum Zweck des Vorweisens eigener Ausweise installiert und eingerichtet haben, dient die eAusweis Check-App.

4 Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

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

Für die Verhältnismäßigkeits- und Erforderlichkeitsprüfung ist zu beachten, dass mit steigendem Umfang der Datenverarbeitung und der damit einhergehenden Intensität des Eingriffs in die Rechte und Freiheiten der betroffenen Personen auch die Anforderungen an die Wertigkeit der mit der Datenverarbeitung verfolgten Zwecke steigen.[52]

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

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

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

- Informationspflichten gegenüber den Betroffenen (Art 12, 13 und 14);
- Auskunftsrecht und Recht auf Datenübertragbarkeit (Art 15 und 20);
- Recht auf Berichtigung und Löschung (Art 16, 17 und 19);
- Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Art 18, 19 und 21);
- Verhältnis zu Auftragsverarbeitern (Art 28);
- Garantien in Bezug auf die internationale Übermittlung von Daten.[53]

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

4.1 Personenbezug

4.1.1 Was sind personenbezogene Daten?

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

Die Definition des Begriffs „personenbezogene Daten" ist somit sehr weit gefasst, denn es werden dem Wortlaut zufolge alle Informationen, die sich auf eine natürliche Person beziehen, davon umfasst.[54] 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.[55] 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.[56]

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[57], IMSI[58], UDID[59], MSISDN[60]), die Identität des Telefons[61], Kreditkarten- und Zahlungsdaten oder auch der Browserverlauf als personenbezogene Daten zu werten sind.[62] Weitere gängige Angaben mit identifizierendem Bezug zu einer natürlichen Person sind zB Handynummer[63], E-Mail-Adresse, Sozialversicherungsnummer[64], KFZ-Kennzeichen[65], IP-Adresse[66] und auch medizinische Diagnosen.[67]

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.[68] 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,

---

[54] *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9 DSGVO (Stand 1. 12. 2018, rdb.at).
[55] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO² Art 4 Nr 1 Rz 8.
[56] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO² Art 4 Nr 1 Rz 8.
[57] *International Mobile Equipment Identity* – eindeutige Nummer des Endgeräts.
[58] *International Mobile Subscriber Identity*– eindeutige Nummer des Netzteilnehmers.
[59] *Unique Device Identifier*– eindeutige Gerätenummer für Apple-Produkte.
[60] *Mobile Station Integrated Services Digital Network* – weltweit eindeutige Mobilfunk-Rufnummer.
[61] 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".
[62] *Artikel-29-Datenschutzgruppe,* Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, WP 202 (2013) 10 f.
[63] *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013, 10.
[64] Vgl DSK 12. 11. 2004, K120.902/0017-DSK/2004; BVwG 11.06.2018, W211 2161456-1.
[65] Vgl VfGH 15. 6. 2007, G 147/06; DSK 11.7.2008, K121.359/0016-DSK/2008.
[66] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[67] *Hödl* in *Knyrim*, DatKomm Art 4 Rz 9 DSGVO.
[68] Vgl *Klabunde* in *Ehmann/Selmayr*, DS-GVO² Art 4 Rz 8.

bei der es sich immer um eine natürliche Person handeln muss. Der vierte und letzte wesentliche Faktor der Begriffsbestimmung „personenbezogener Daten" ist die Identifizierung bzw Identifizierbarkeit. Bei der vorliegenden Identitätskomponente bedarf es einer klaren Abgrenzung zwischen den sogenannten „*primären Identifikationsmerkmalen*" und jenen Daten, die für die Identifizierbarkeit einer natürlichen Person geeignet sind.

Informationen, aus denen die Identität der Person unmittelbar hervorgeht, werden als „*primäres Identifikationsmerkmal*" bezeichnet.[69] 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.[70] Dies hat zur Folge, dass sämtliche weiteren Informationen, die direkt einer identifizierten Person zuordenbar sind, als personenbezogene Daten gem Art 4 Z 1 DSGVO zu werten sind.

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

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

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

Die Literatur[71] und unionsrechtliche Judikatur[72] setzen am sogenannten „*relativen Personenbezug"* bzw der "*relativen Theorie*"[73] an, wonach für die Bestimmung der Identifizierbarkeit die Kenntnisse und Mittel der datenverarbeitenden Stelle und nicht irgendeines *Dritten* ausschlaggebend sind. Sofern

[69] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[70] *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.
[71] 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.
[72] Vgl EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779.
[73] Vgl *Hödl* in *Knyrim,* DatKomm Art 4 Rz 14; *Klar/Kühling* in *Kühling/Buchner* DS-GVO/BDSG[2] Art 4 Nr 1 Rz 26 ff; *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.

der *Verantwortliche* Einzelangaben einer Person durch relevantes Zusatzwissen[74] [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.[75] 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.*"[76]

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 3.2) aufgelisteten Datenkategorien von personenbezogenen Daten auszugehen, zumal die datenverarbeitende Stelle in aller Regel einen Personenbezug im Sinne der Ausführungen dieses Kapitels herstellen können wird.

Anzumerken ist in diesem Zusammenhang außerdem, dass der Personenbezug von Daten auch durch ein Verschlüsselungsverfahren nicht geschmälert wird, weil die datenverarbeitende Stelle auch weiterhin den Personenbezug herstellen kann.[77] 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,[78] und daher zum Schutz personenbezogener Daten wesentlich beiträgt. Dementsprechend sind im gegebenen Fall jedenfalls auch verschlüsselte Daten, soweit solche unter 3.2 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.

[74] 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).
[75] Vgl *Eßer* in *Eßer/Kramer/v.Lewinski*, DSGVO/BDSG[7] Art 4 Rz 20.
[76] EuGH C-582/14, *Breyer*, ECLI:EU:C:2016:779, Rz 65.
[77] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.
[78] *Klabunde* in *Ehmann/Selmayr*, DS-GVO[2] Art 4 Rz 19.

4.2 Rechtsgrundlagen

4.2.1 Regelungssystematik der DSGVO

Die aus der DSGVO abzuleitende Regelungssystematik in Bezug auf die Rechtsgrundlagen sieht vor, dass jegliche Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, ein Erlaubnistatbestand bzw eine Rechtsgrundlage der Art 6, 9 bzw 10 DSGVO rechtfertigt die betreffende Datenverarbeitung.[79] Für die 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[80] (kurz: sensibler Daten) gestützt werden kann.

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

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

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

4.2.2 Initiale Anmeldung an der eAusweise-App und Einrichtung

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

Eine solche Rechtsgrundlage muss dabei durch Unionsrecht oder das Recht des betreffenden Mitgliedstaats festgelegt werden, dem der *Verantwortliche* unterliegt. Art 6 Abs 1 lit e steht in einem engen Zusammenhang mit Art 6 Abs 2 und 3, wonach der Zweck zur Erfüllung der gesetzlich übertragenen Aufgabe notwendig sein muss. Letztere muss in der Rechtsgrundlage hinreichend bestimmt beschrieben werden. Da Art 6 Abs 1 lit e ein sehr weit gefächertes Anwendungsspektrum besitzt, ist laut Artikel-29-Datenschutzgruppe *„eine strenge Auslegung und eine klare Benennung des gegebenen öffentlichen Interesses und der öffentlichen Gewalt, die die Verarbeitung rechtfertigen, auf Einzelfallbasis geboten.“*[81]

Die nationalen Rechtsgrundlagen sind die §§ 4 iVm 4b iVm 2 Z 10 iVm 2 Z 10a, § 14 Abs 3 und § 14a Abs 2 E-GovG. Diese Datenverarbeitung ist ein konkreter Anwendungsfall der Verarbeitungstätigkeit “Verwendung der ID Austria” des ID Austria Systems. Es erfolgt keine Übermittlung zusätzlicher Attribute bzw Merkmale iSd § 4 Abs 2 E-GovG, weshalb keine Einwilligung einzuholen ist. Die Übermittlung des Minimaldatensatzes inklusive bPK ist durch §§ 4 Abs 5 iVm 4b Abs 1 E-GovG gedeckt.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[82] aus:

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

Die qualifizierte Signatur wird bei der Smartphone-basierten Umsetzung des Bürgerkartenkonzepts (so genannte Handy-Signatur) aktuell durch drei Faktoren ausgelöst, das Wissen des Benutzers (Passwort – Faktor 1), der Besitz des Geräts (hardwarebasiertes Element für Schlüsselaufbewahrung – Faktor 2) und eine biometrische Eigenschaft des Benutzers (aktuell Fingerabdruck und bestimmte Gesicht-Scans – Faktor 3). Der sicherheitstechnisch gleichwertige Vorgang zum Auslösen der Erstellung einer Personenbindung bei Verwendung des E-ID wird erstmalig durch eine qualifizierte Signatur des E-ID-Inhabers initiiert. Dabei wird als Sicherheitselement ein Schlüssel im hardwarebasierten Element des Geräts erstellt und der Zugriff mit einer biometrischen Eigenschaft abgesichert (äquivalent zum zweiten und dritten Faktor der qualifizierten Signatur) und durch den E-ID-Inhaber qualifiziert signiert. Dadurch entsteht

[81] Vgl *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 45 ff (Stand 7. 5. 2020, rdb.at).
[82] ErläutRV 469 BlgNR 27. GP 2.

eine kryptographische Bindung zwischen der qualifizierten Signatur des E-ID-Inhabers und dem erstellten Schlüssel. Die Kombination aus der kryptographischen Bindung durch die initial erstellte qualifizierte Signatur und der Verwendung des zuvor erwähnten Sicherheitselements entspricht einem sicherheitstechnisch gleichwertigen Vorgang. Das zugehörige qualifizierte Zertifikat, das für die frühere qualifizierte elektronische Signatur verwendet wurde, muss zum Zeitpunkt der jeweiligen Verwendung gültig sein.

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

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

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

Zudem führen die Materialien[83] aus:

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

Die Verarbeitung der unter 3.2.1 genannten Daten stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationale Rechtsgrundlage bildet § 15a FSG iVm § 16a Abs 1 Z 1 lit a bis c und f FSG iVm § 16a Abs 1 Z 3 lit a bis g FSG.

4.2.3 Führerschein laden

Die Datenverarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationalen Rechtsgrundlagen bilden die §§ 15a Abs 2 und 5 iVm § 16a Abs1 Z 1 lit a bis c und f iVm § 16a Abs 1 Z 3 lit a bis g FSG.

§ 15a Abs 2 FSG regelt hierbei den Zugriff des *E-ID-Inhabers* auf das Führerscheinregister, § 15a Abs 5 FSG ist die Rechtsgrundlage beim Zugang der Stammzahlregisterbehörde, sohin des BMF.[84]

[83] ErläutRV 469 BlgNR 27. GP 7.

[84] Anlage zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG), BGBl I 1986/76 idF BGBl I 2022/98; siehe erläuternd: https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 23. 8. 2022).

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[85] aus:

„Der Führerscheinbesitzer hat auch die Möglichkeit einer Selbstabfrage im Führerscheinregister. Dabei werden die wesentlichen persönlichen Daten geliefert (Name, Geburtsdatum, akademischer Grad) sowie die relevanten Führerscheindaten, die auch im Dokument ersichtlich sind (Ausstellungsbehörde, erteilte Klassen, Erteilungsdatum, Ausstellungsdatum des Führerscheines, Antragsnummer, Foto und auch Auflagen und Befristungen).

…

§ 4 Abs. 5 letzter E-GovG (bzw. in weiterer Folge auch § 4 Abs. 6 E-GovG) knüpft sowohl an die technische als auch datenschutzrechtliche Zugänglichkeit von Registern an. Mit Abs. 5 soll dementsprechend für die Stammzahlenregisterbehörde die datenschutzrechtliche Grundlage für den Zugang zum Führerscheinregister und somit auch für die Abfrage der in Abs. 2 genannten Daten erfolgen.“

4.2.4 Verkehrskontrolle

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 § 15a Abs 1 FSG dar. Durch die in Gestalt der soeben zitierten Norm nunmehr existierende Alternative verfügen Führerscheinbesitzer*innen faktisch über zwei Nachweismöglichkeiten einer Lenkberechtigung, nämlich einerseits in Form des „digitalen“ Führerscheins sowie andererseits mittels des klassischen physischen Führerscheins.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[86] aus:

“Diese Bestimmung enthält die grundsätzliche Regelung und legt die Rahmenbedingungen für die Nutzung des „digitalen“ Führerscheines fest. Voraussetzung ist das Vorliegen eines Lichtbildes iSd § 16a Abs. 1 Z 3 lit. f FSG im Führerscheinregister, da im Zuge einer Kontrolle die Identität des Inhabers des Führerscheines an Hand der durch das Führerscheinregister abgefragten Daten festgestellt werden muss. Diese Voraussetzung liegt nur dann vor, wenn der Inhaber der Lenkberechtigung über einen Scheckkartenführerschein verfügt. Da für die digitale Kontrolle des Führerscheines eine Online-Verbindung zum Führerscheinregister und damit eine mobile Verfügbarkeit einer Internetverbindung am Ort der Kontrolle erforderlich ist, müssen die Rechtsfolgen für den Fall einer fehlenden Internetverbindung sowie für den Fall, dass das Endgerät des Nutzers nicht funktionsfähig ist (schadhaftes Gerät, leerer Akku etc…), geregelt werden. Abs. 1 überträgt dieses Risiko generell auf den Nutzer des Systems, er wird in solchen Fällen so behandelt werden, wie wenn der Führerschein nicht mitgeführt wird. Für die Straßenkontrollen von Führerscheinen ist somit jedenfalls eine Online-Verbindung zum Führerscheinregister erforderlich, daneben gibt es für andere Zwecke aber auch eine offline-Speicherung von gewissen Führerscheindaten, deren Rahmenbedingungen in Abs. 4 geregelt werden.”

Im Rahmen einer Verkehrskontrolle verarbeiten Sicherheitsorgane Führerscheindaten bzw Führerscheinregisterdaten. Im Zuge der Nutzung des digitalen Führerscheins anfallende Verarbeitungen stützen sich hierbei grundsätzlich auf dieselben bewährten Rechtsgrundlagen wie im Fall des physischen Führerscheins. Die Verarbeitung der Führerscheindaten, also die Aushändigung, wird hierbei durch Art

[85] ErläutRV 469 BlgNR 27. GP 11,12.
[86] ErläutRV 469 BlgNR 27. GP 11.

6 Abs 1 lit e DSGVO iVm § 14 Abs 1 FSG legitimiert. Die Einschau ins Führerscheinregister stützt sich auf Art 6 Abs 1 lit e DSGVO iVm § 16 Abs 3 FSG.

Die Sicherungsmaßnahme einer vorläufigen Abnahme des digitalen Führerscheins stützt sich auf den neu geschaffenen § 39 Abs 1a FSG und sohin auf eine andere Rechtsgrundlage als dies bei einem mitgeführten Scheckkartenführerschein der Fall ist.

Hierzu führen die Materialien[87] aus:

"Da im Nutzungsfall des „digitalen" Führerscheins auch die Mitführverpflichtung des Scheckkartenführerscheines entfällt, ist es zur Erhaltung der Sicherungsmaßnahme einer vorläufigen Abnahme des Führerscheines notwendig, dass dann wenn die Voraussetzungen einer vorläufigen Abnahme des Führerscheines vorliegen, dieser Umstand, unabhängig davon ob eine Führerscheinabnahme faktisch erfolgen kann oder nicht, durch das einschreitende Organ des öffentlichen Sicherheitsdienstes oder der Straßenaufsicht in das Führerscheinregister eingetragen und gleichzeitig gegenüber dem Betroffenen vom Organ, auf das Verbot des Lenkens eines Fahrzeuges, durch Ausfolgung einer Bescheinigung hingewiesen wird. Im Führerscheinregister wird die Möglichkeit geschaffen, damit die Exekutive das Vorliegen der Voraussetzungen der vorläufigen Abnahme des Führerscheines eintragen kann. Mit den vorliegenden Änderungen wird die vorläufige Abnahme eines Führerscheines der Feststellung der Voraussetzungen zur vorläufigen Abnahme des Führerscheines durch das einschreitende Organ des öffentlichen Sicherheitsdienstes oder der Straßenaufsicht und Bescheinigung dieses Umstandes an den Betroffenen gleichgestellt. Durch die Gleichstellung beseitigt die Novelle zur Nutzung des „digitalen" Führerscheines bestehende Kontrolldefizite und wird damit die Nachweissicherheit der Dokumente „digitaler" und Scheckkartenführerschein durch zeitgleiche Eintragung im Führerscheinregister, auch im Rechtsverkehr gegenüber Dritten, wie dem Zulassungsbesitzer, im Falle eines Überlassens von Kraftfahrzeugen, gesteigert."

4.2.5 Ausweis offline vorweisen (außer Verkehrskontrolle)

Die Datenverarbeitung stützt sich auf Art 6 Abs 1 lit e DSGVO (allenfalls Art 9 Abs 2 lit g DSGVO). Die nationalen Rechtsgrundlagen bilden die §§ 15a Abs 3, 4 und 5 FSG iVm § 16a Abs 1 Z 1 lit a bis c und f FSG iVm § 16a Abs 1 Z 3 lit a bis g FSG.

Zur Zweckbestimmung und Notwendigkeit führen die Materialien[88] aus:

"Auch die Ausweisfunktion oder der Lenkberechtigungsnachweis gegenüber dritten Personen oder Unternehmen wird ermöglicht. Es werden die gleichen Daten übermittelt, wie bei der Selbstabfrage, mit Ausnahme von Auflagen oder Beschränkungen unter denen die Lenkberechtigung erteilt wurde. Befristungen werden im Hinblick auf die Verpflichtungen des Zulassungsbesitzers sich über das Bestehen einer erforderlichen Lenkberechtigung zu überzeugen, hingegen schon geliefert, da dieser Umstand in gewissen Situationen wichtig sein kann. So muss etwa ein Autovermieter ersehen können, ob die Lenkberechtigung des Mieters für die gesamte Mietdauer aufrecht, ist.

[...]

[87] ErläutRV 469 BlgNR 27. GP 12.
[88] ErläutRV 469 BlgNR 27. GP 11, 12.

In diesem Absatz wird die „offline"-Speicherung der Führerscheindaten geregelt („Nachweis in vereinfachter Form"). Dieser Nachweis darf aber nur für andere Zwecke als für den Nachweis der Lenkberechtigung verwendet werden, etwa wenn der Nutzer des Systems den digitalen Führerschein als reinen Lichtbildausweis zum Nachweis seiner Identität verwenden will (z. B. bei Briefabholung am Postamt, Nachweis der Vollendung eines gewissen Mindestalters etc.). Muss hingegen gegenüber Dritten der aufrechte Besitz der Lenkberechtigung nachgewiesen werden (gegenüber dem Arbeitgeber oder bei Übernahme eines Mietwagens), darf diese Offline-Funktion nicht zum Nachweis der Lenkberechtigung verwendet werden. Die offline-Speicherung wird aus Gründen der Sicherstellung der Datenaktualität nach drei Monaten ungültig und muss unter Nutzung einer Onlineverbindung und Verwendung des E-ID durch einen erneuten Abgleich mit dem Führerscheinregister aktualisiert werden. Die eingeschränkte Verwendbarkeit dieser offline-Version sowie der Zeitpunkt der letzten Aktualisierung ist in der Applikation deutlich zu kennzeichnen, um Missverständnissen aber auch der missbräuchlichen Verwendung vorzubeugen."

Auch hier stellt § 15a Abs 5 FSG die Rechtsgrundlage für den Zugang des BMF als Stammzahlenregisterbehörde zu den in § 15a Abs 2 FSG genannten Daten dar.[89]

Auch an dieser Stelle ist auf die Materialien[90] zu verweisen:

"§ 4 Abs. 5 letzter [Anm, richtig: Satz] *E-GovG (bzw. in weiterer Folge auch § 4 Abs. 6 E-GovG) knüpft sowohl an die technische als auch datenschutzrechtliche Zugänglichkeit von Registern an. Mit Abs. 5* [Anm: § 15a Abs 5 FSG] *soll dementsprechend für die Stammzahlenregisterbehörde die datenschutzrechtliche Grundlage für den Zugang zum Führerscheinregister und somit auch für die Abfrage der in Abs. 2 genannten Daten erfolgen."*

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

4.2.6 Widerruf des Gerätezertifikats AWP

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

Zur Zweckbestimmung und Notwendigkeit führen die Materialien aus:[91]

„Die Registrierung des E-ID erfolgt stets unter Verarbeitung personenbezogener Daten in der zentralen Evidenz, die Registrierungsdaten sind dem qualifizierten VDA zur Ausstellung eines qualifizierten Zertifikats zu übermitteln. E-ID-Inhaber haben das Recht, zu jedem Zeitpunkt eine vorübergehende Aussetzung sowie einen Widerruf des E-ID bei der Behörde zu verlangen. § 4a Abs. 5 verpflichtet die Behörden

[89] Anlage zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG), BGBl I 1986/76 idF BGBl I 2022/98; siehe erläuternd: https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 23. 8. 2022).
[90] ErläutRV 469 BlgNR 27. GP 12.
[91] ErläutRV 469 BlgNR 27. GP 4.

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

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

4.2.7 Abmelden von der eAusweise-App

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

4.2.8 Überprüfen des Ausweises in der eAusweise-App

Technische Voraussetzung für die Verwendung der eAusweise-App generell und somit auch für deren Verwendung zur Überprüfung von Ausweisen ist, dass sich die überprüfende Person, wie unter 3.2.1 beschrieben, zum dort angegebenen Zweck an der eAusweise-App angemeldet hat.[92] Darüber hinaus werden im Zuge eines Überprüfungsvorgangs keine personenbezogenen Daten der überprüfenden Person verarbeitet, weshalb keine datenschutzrechtliche Rechtsgrundlage erforderlich ist.

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

4.2.9 eAusweis Check-App

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

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

[92] Zum Überprüfen von Ausweisen durch Nutzer*innen, die nicht bereits die eAusweise-App zum Zweck des Vorweisens eigener Ausweise installiert und eingerichtet haben, dient die eAusweis Check-App.

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;[93] 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*"[94] 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.[95]

Sofern jedoch zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, führt dies zur sogenannten "*pluralistische*[n] *Kontrolle*"[96] 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*"[97] 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,[98] 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.[99]

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:

---

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

- *Namen und Kontaktdaten aller Verantwortlichen;*[100]
- *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;*[101]
- *gegebenenfalls Benennung eines Verantwortlichen als zentrale Anlaufstelle nach Art 26 Abs 1 S 3*.[102]

An der jeweiligen Verarbeitung kann auch ein ***Auftragsverarbeiter*** mitwirken, der dem *Verantwortlichen* stets als „*verlängerter Arm*“[103] dient. Dies, da der *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, als rechtlich eigenständige und externe Organisation,[104] Datenverarbeitungstätigkeiten lediglich „im Auftrag“ des *Verantwortlichen* durchzuführen hat. Daher kommt dem *Auftragsverarbeiter* grds keine Entscheidungsbefugnis hinsichtlich der Verarbeitungszwecke und (wesentlichen) -mittel zu.[105] 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.[106] Jedoch liegt die Entscheidungskompetenz über die „wesentlichen Mittel“ der Verarbeitung stets beim *Verantwortlichen*.[107]

Die dem *Verantwortlichen* oder *Auftragsverarbeiter* unterstellten Personen gelten grds als ihnen „*zurechenbare Personen*“[108], da sie idR nur als „*Ausführungsorgan*“ für den *Verantwortlichen* oder *Auftragsverarbeiter* tätig sind.[109] Dies gilt jedoch nur solange sie sich an die Vorgaben bzw vorab festgelegten Zwecke und Mittel der Verarbeitung halten.

---

[100] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Bertermann* in *Ehmann/Selmayr,* DS-GVO² Art 26 Rz 12; *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG² Art 26 Rz 9.
[101] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41 unter Verweis auf *Veil* in *Gierschmann/Schlender/Stentzel/Veil,* DS-GVO Art 26 Rz 64.
[102] *Horn* in *Knyrim,* DatKomm Art 26 Rz 41.
[103] *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter – was ändert sich mit der DSGVO? ZTR 2017, 59 (59).
[104] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 30.
[105] Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 94.
[106] *Hartung* in *Kühling/Buchner*, DS-GVO/BDSG² Art 4 Nr 7 Rz 13; *Feiler/Forgó*, EU-DSGVO Art 4 Anm 12; *Artikel-29-Datenschutzgruppe,* Stellungnahme 1/2010, 17.
[107] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010, 17 f.
[108] 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.
[109] *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,[110] der zumindest ein „gewisses Maß an Eigenständigkeit“[111] aufzuweisen hat und dem personenbezogene Daten innerhalb einer Verarbeitungstätigkeit lediglich offengelegt werden.

Ferner gibt es auch die Rolle des „außenstehenden“[112] ***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.[113] Es kann daher jeder lebende[114] Mensch die Rolle der betroffenen Person einnehmen, unabhängig von einer spezifischen Voraussetzung iS eines bestimmten Alters oder Geisteszustands.[115]

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.[116] 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.[117]

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.[118]

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

---

[110] 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,* (…).“

[111] 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.

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

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

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

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

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

[117] 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.*“

[118] 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.

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

in den einfachgesetzlichen Bestimmungen des DSG auch juristische Personen erfasst.[120] 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.[121]

4.3.2 Abgrenzungskriterien für die Ermittlung der (gemeinsam) Verantwortlichen

Basierend auf der bisherigen und maßgeblichen Rechtsprechung[122] 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.[123]
- 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.[124]
- Gemeinsame Verantwortlichkeit setzt nicht voraus, dass sämtliche Verantwortliche für dieselbe Verarbeitungstätigkeit einen (gemeinsamen) Zugang zu den betreffenden personenbezogenen Daten haben müssen.[125]
- Im Umkehrschluss kann dies jedoch bedeuten, dass, sofern mehrere Verantwortliche, die gemeinsam personenbezogene Daten erheben bzw verarbeiten, darüber hinaus auch über einen gemeinsamen Zugang zu den betreffenden personenbezogenen Daten verfügen, die Qualifikation derer als gemeinsam Verantwortliche naheliegt.
- Das Bestehen einer gemeinsamen Verantwortlichkeit hat nicht zwangsläufig eine gleichwertige Verantwortlichkeit sämtlicher Verantwortlichen für dieselbe Verarbeitungstätigkeit zur Folge.[126] Daher kann die Verantwortlichkeit bestimmter Verantwortlicher in verschiedenen

[120] *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.
[121] *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).
[122] EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317; EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388; EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551; EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.
[123] EuGH C-131/12, *Google Spain und Google*, ECLI:EU:C:2014:317, Rz 34.
[124] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 36 ff, 39.
[125] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 38.
[126] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.

Phasen und in unterschiedlichem Ausmaß ausgeprägt sein, wodurch der Grad der Verantwortlichkeit variieren kann.[127] 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.[128]
- 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.[129]
- Für die Entscheidung über Zwecke und Mittel der Verarbeitung bedarf es keiner schriftlichen Anleitung oder Anweisung zur gemeinsamen Datenverarbeitung.[130]
- Eine gemeinsame Entscheidung über das Mittel der Verarbeitung (wie Social Plug-In[131]) 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.[132]
- 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.[133]
- 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.[134]

[127] EuGH C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn 43.
[128] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 68, 70 ff.
[129] Vgl EuGH C-25/17 VbR 2018/110 (202).
[130] EuGH C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, Rn 67.
[131] 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.
[132] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 77, 79.
[133] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 80 ff, 84.
[134] EuGH C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, Rn 74, 85.

4.3.3 Rollenverteilung der Ausweisplattform - Digitaler Führerschein

Für die Rollenverteilung in der Ausweisplattform, vor allem im Hinblick auf die Rolle des oder der *Verantwortlichen*, kommt in Zusammenschau des E-GovG mit dem FSG zunächst der sogenannten "*rechtlichen Verantwortlichkeit*"[135] 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,[136] oder konkrete Verarbeitungstätigkeiten zugewiesen werden können, woraus sich basierend auf deren expliziter Zuständigkeit hierfür ihre rechtliche Verantwortlichkeit betreffend der mit den zugewiesenen Aufgaben einhergehenden Verarbeitung von personenbezogenen Daten ergeben kann.

In Anbetracht des Beurteilungsaspekts der rechtlichen Verantwortlichkeit ist vor allem § 44 Abs 5 FSG einschlägig. Dieser betraut die Bundesministerin für Digitalisierung und Wirtschaftsstandort mit der Vollziehung des § 15a FSG, welcher seinerseits die Umsetzung des digitalen Führerscheines regelt.

Die Materialien führen erläuternd aus:

"Als federführend zuständiges Ressort für die Umsetzung der digitalen Maßnahmen dieser Novelle wird die Bundesministerin für Digitalisierung und Wirtschaftsstandort mit der Vollziehung der §§ 15a und 43 Abs. 29 dieser Novelle betraut."

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"[137], zumal die vollumfängliche Verantwortung über eine Datenverarbeitung nur jener Akteur trägt, der über die Zwecke und Mittel der Verarbeitung entscheidet.[138] Diesbezüglich ist hervorzuheben, dass das BMF Stammzahlregisterbehörde ist[139] und sohin nach § 15a Abs 5 FSG Zugang zu Führerscheinregisterdaten hat und im Rahmen des gesetzlichen Auftrages auch wesentlichen faktischen Einfluss auf die Systemausgestaltung nimmt.

4.3.4 Initiale Anmeldung an der eAusweise-App und Einrichtung

Die Nutzer*in führt mithilfe der ID Austria einen Anmeldevorgang durch. Das BMF agiert für das Service eAusweise-App als Service Owner iSd ID Austria. Das BMF ist bezüglich des Datenverkehrs zur Nutzer*in als *Verantwortlicher* iSd Art 4 Z 7 DSGVO zu qualifizieren, da es im Rahmen des Auftrages des § 44 Abs 5 FSG den Betrieb der Anmeldeschnittstelle beauftragt. Zusätzlich ist das BMF der Verantwortliche für die Verwendung des E-ID zur Anmeldung.

---

[135] *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (110); *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG² Art 4 Nr 7 Rz 15.
[136] Vgl *Raschauer* in *Sydow,* Europäische Datenschutzgrundverordnung² Art 4 Rz 141; *Hartung* in *Kühling/Buchner,* DS-GVO/BDSG² Art 4 Nr 7 Rz 14.
[137] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83.
[138] *Hödl* in *Knyrim,* DatKomm Art 4 Rz 83; *Buder* in *Jahnel* (Hrsg), Datenschutzrecht, 97 (101).
[139] Anlage zu § 2 Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien BGBl I 1986/76 idF BGBl I 2022/98; siehe erläuternd: https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 23. 8. 2022).

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BMF des BRZ als *Auftragsverarbeiter* gem Art 4 Z 8 DSGVO, denn das BRZ betreibt die Anmeldeschnittstelle (eAusweise-App[140]). Diese Verarbeitung erfolgt im Rahmen eines Vertragswerks, abgeschlossen zwischen der BRZ GmbH und der Republik Österreich, dessen Bestandteil auch ein Auftragsverarbeitungsvertrag nach Art 28 DSGVO ist.

Verantwortlicher:

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

Auftragsverarbeiter:

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

4.3.5 Führerschein laden

Die datenschutzrechtliche Verantwortlichkeit des BMF stützt sich ebenfalls auf § 44 Abs 5 FSG. Das BMF ist auch faktisch federführend an der Parametrierung der eAusweise-App beteiligt und beauftragt den Betrieb der Schnittstelle zwischen Bürger und Führerscheinregister, weshalb das BMF insgesamt als verantwortliche Stelle zu qualifizieren ist.

Im Rahmen dieser Verarbeitungstätigkeit bedient sich das BMF des BRZ als *Auftragsverarbeiter*, welcher im Auftrag des BMF die Schnittstelle zwischen Führerscheinregister und Nutzer*innen betreibt.

Gemäß § 16 Abs 1 Z 1 FSG ermitteln und verarbeiten die in § 16b Abs 2 und 3 FSG genannten Behörden[141] in mittelbarer Bundesverwaltung die personenbezogenen Daten im Führerscheinregister im gesetzlichen Auftrag eigenverantwortlich und werden insoweit als datenschutzrechtlich Verantwortliche tätig.

Zur Möglichkeit einer gemeinsamen Verantwortlichkeit mit dem BMF siehe 4.3.6.

Verantwortliche:

- BMF: Betrieb Ausweisplattform
- Führerscheinbehörden: datenschutzrechtliche Verantwortlichkeit für die in mittelbarer Bundesverwaltung im gesetzlichen Auftrag eigenverantwortlich verarbeiteten personenbezogenen Daten im Führerscheinregister

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.6 Verkehrskontrolle

Da das BMF an diversen Stellen an den Datenverarbeitungen beteiligt ist, ist zu prüfen, ob dessen organisierende und koordinierende Tätigkeiten[142] eine gemeinsame Verantwortlichkeit mit den Führerscheinbehörden sowie BMI bzw den LPD oder den Gemeinden begründen. Konkret verantwortet das

[140] Die eAusweise-App agiert als Service Provider im Rahmen der ID Austria. Siehe Abschnitt 3.2.1.
[141] Also jene Behörden, die mit der Verfahrensführung in Führerscheinangelegenheiten betraut sind, konkret daher Bezirkshauptmannschaften und Landespolizeidirektionen.
[142] Vgl EuGH 10. 7. 2018, C-25/17, *Jehovan todistajat*, Rz 73.

BMF 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 Verkehrskontrolle 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 BMF an den im Rahmen der Verkehrskontrolle anfallenden Daten erschöpft sich darin, dass es Rahmenbedingungen schafft, um Bürger*innen Dienste im Rahmen des gesetzlichen Auftrages (vgl § 44 Abs 5 FSG) 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, im Zuge einer Verkehrskontrolle den Führerschein in digitaler Form vorzuweisen, bei der jeweiligen betroffenen Person selbst liegt, weil diese stets frei zwischen digitalem Führerschein und physischem Führerschein wählen kann. Umgekehrt eröffnet das BMF Bürger*innen unabhängig vom BMI bzw den LPD sowie den Gemeinden die Möglichkeit, Führerscheindaten digital vorzuweisen. BMI, LPD und Gemeinden haben hierbei keinen Einfluss auf die Parametrierung.

Die Gemeinde ist als verantwortliche Stelle hinsichtlich der in der GWK Check-App durch das Gemeindeorgan verarbeiteten Daten zu qualifizieren, sohin für die Nutzung der GWK Check-App.

Selbige Überlegungen gelten auch für das Verhältnis der Führerscheinbehörden als verantwortliche Stellen hinsichtlich der im Führerscheinregister eingetragenen personenbezogenen Daten zum BMF im Rahmen seines gesetzlichen Auftrages. So hat das BMF weder faktischen Einfluss auf die im Führerscheinregister eingetragenen personenbezogenen Daten noch liegt eine rechtliche Verantwortlichkeit vor. Zwar kann das BMF nach Maßgabe des § 15a FSG auf bestimmte Daten des Führerscheinregisters zugreifen bzw den Zugriff ermöglichen, es hat jedoch keinen Einfluss darauf, welche Daten im Register anfallen und wie diese gehalten werden. Eine Zugriffsmöglichkeit für sich sollte keine gemeinsame Verantwortlichkeit begründen.

Im Übrigen ist auf die bereits in Punkt 4.3.5 enthaltenen Ausführungen betreffend die Verantwortlichkeiten für personenbezogene Daten im Zusammenhang mit § 16b Abs 2 und 3 FSG zu verweisen.

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

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

Verantwortliche:

- BMF: Betrieb Ausweisplattform, Betrieb GWK Check-App
- BMI bzw LPD: Organe des öffentlichen Sicherheitsdienstes ausgenommen Gemeindewachkörper
- Gemeinden: Gemeindewachkörper, Nutzung GWK Check-App

- Führerscheinbehörden: datenschutzrechtliche Verantwortlichkeit für die in mittelbarer Bundesverwaltung im gesetzlichen Auftrag eigenverantwortlich verarbeiteten personenbezogenen Daten im Führerscheinregister[143]

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform, Betrieb GWK Check-App

4.3.7 Ausweis offline vorweisen (außer Verkehrskontrolle)

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.

Das BMF ist bezüglich des Datenverkehrs zur Nutzer*in als *Verantwortlicher* iSd Art 4 Z 7 DSGVO zu qualifizieren, da es im Rahmen des Auftrages des § 44 Abs 5 FSG die Schnittstelle für den Datenaustausch betreibt.

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[144] des BMF ist das Vorliegen einer gemeinsamen Verantwortlichkeit zwischen überprüfender Person und BMF zu erwägen. Die überprüfende Person entscheidet jedoch autonom, ob sie einen Prüfungsvorgang startet und verfolgt daneben eigenständige, auf konkrete Beziehungen zur Nutzer*in gerichtete Interessen. Das BMF hat weder unmittelbare noch mittelbare Interessen an den konkreten verarbeiteten Daten oder den Verarbeitungszwecken. Somit liegt auch hier keine gemeinsame Verantwortlichkeit vor.

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 keine datenschutzrechtliche Rolle zu.

Verantwortliche:

- BMF: Betrieb Ausweisplattform
- Überprüfende Person: Überprüfung des Führerscheins für jeweils eigene Zwecke

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.8 Widerruf des Gerätezertifikats AWP

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

Verantwortlicher:

[143] Siehe Abschnitt 4.3.5.
[144] Vgl EuGH 10. 7. 2018, C-25/17, *Jehovan todistajat*, Rz 73.

- BMF: Betrieb Ausweisplattform

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.9 Abmelden von der eAusweise-App

Es liegt dieselbe Rollenverteilung vor wie bei der Verarbeitungstätigkeit „Initiale Anmeldung an der eAusweise-App und Einrichtung“ (4.3.4).

Verantwortlicher:

- BMF: Betrieb Ausweisplattform

Auftragsverarbeiter:

- BRZ: Betrieb Ausweisplattform

4.3.10 Überprüfen des Ausweises in der eAusweise-App

Da sich die überprüfende Person in der eAusweise-App über die ID Austria anmeldet, liegt dieselbe Rollenverteilung vor wie bei der Verarbeitungstätigkeit „Initiale Anmeldung an der eAusweise-App und Einrichtung”. Für genaue Angaben zur Rollenverteilung siehe daher unter 4.3.4. Zur Verarbeitung personenbezogener Daten der zu überprüfenden Person siehe insbesondere unter 4.3.7.

Verantwortlicher:

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

Auftragsverarbeiter:

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

4.3.11 eAusweis Check-App

Es liegt keine Verarbeitung personenbezogener Daten der die eAusweis Check-App nutzenden überprüfenden Person vor und daher ist diesbezüglich keine datenschutzrechtliche Rolle zu qualifizieren. Zur Verarbeitung personenbezogener Daten der *zu überprüfenden* Person siehe insbesondere unter 4.3.7.

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.[145] 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.[146]

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 3.2 dokumentiert. Dort finden sich auch Begründungen für die Erforderlichkeit, soweit es solcher bedarf.

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

- Die betroffene Person kann frei entscheiden, ob sie digitale Ausweise verwendet oder ausschließlich physische Ausweise.
- In jedem einzelnen Fall kann die betroffene Person frei entscheiden, wem sie ihren digitalen Ausweis vorweist und nur in diesem Fall kommt es zur Übermittlung personenbezogener Daten, die überdies direkt zwischen den Endgeräten ohne Einbeziehung eines Servers erfolgt.[147]
- Der digitale Führerschein ist der erste eingeführte Anwendungsfall der Ausweisplattform. Die Daten, die die Nutzer*in des digitalen Führerscheins einem *Dritten* aus der Gesamtheit der im FSR gespeicherten Daten zur Verfügung stellen kann, sind durch den Gesetzgeber in § 15a Abs 3 FSG auf jene beschränkt, die zum Zweck des Nachweises der Lenkberechtigung erforderlich sind. Die betroffene Person kann frei entscheiden, ob sie den digitalen Führerschein auch zum Zweck des Nachweises der Identität oder des Alters verwendet. In diesen Fällen kommt es zu einer über den Zweck hinausgehenden Offenlegung von Daten, und zwar des Ausstellungsdatums, des Datum bzw der Klassen der (nicht) bestehenden Lenkberechtigung sowie des Geburtsorts. Festzuhalten ist, dass dies keine Risikoerhöhung gegenüber der Verwendung des physischen Führerscheins darstellt.

[145] Siehe zudem die primärrechtliche Grundlage in Art 8 Abs 2 EU-Grundrechte-Charta (GRC).
[146] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DSGVO (2018) 37.
[147] Wie in Abschnitt 3.2.3 beschrieben, gilt dies nicht für den Fall der Verkehrskontrolle. Zu beachten sind allerdings die bereits bisher bestehenden Befugnisse der Sicherheitsbehörden zum direkten Zugriff auf die Daten des Führerscheinregisters, die durch das Projekt digitaler Führerschein unberührt bleiben.

- Die überprüfende Person kann frei entscheiden, die anonyme eAusweis Check-App zu verwenden, sodass es zu keiner Verarbeitung ihrer personenbezogenen Daten kommt.

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.

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

Initiale Anmeldung an der eAusweise-App und Einrichtung

Wie unter 3.2.1 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit die Einrichtung der eAusweise-App auf dem Endgerät der Nutzer*in, sodass sie dieser für die Verwendung zur Verfügung steht.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Verschlüsselte Speicherung sowohl der Daten in der Ausweisplattform als auch der Daten auf dem Endgerät
- Grundsätzlich rein automatisierte Verarbeitung, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt

Führerschein laden

Wie unter 3.2.2 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit, den digitalen Führerschein auf das Endgerät der Nutzer*in zu laden.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Vor dem Laden des digitalen Führerscheins 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 Führerscheins, womit auch einer potenziell zweckwidrigen, serverseitigen Verarbeitung vorgebeugt wird
- Verschlüsselung der in der eAusweise-App gespeicherten Daten
- Daten, die für die Funktionen der App benötigt werden, werden nur im lokalen App-Speicher verwendet und nicht zu iCloud oder äquivalenten Systemen übertragen.
- Die Protokollierung ist auf das technisch notwendige Minimum beschränkt, insbesondere werden Vorgänge des Vorweisens und Überprüfen von Ausweisen im System der Ausweisplattform nicht protokolliert.
- Grundsätzlich rein automatisierte Verarbeitung, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen

Verkehrskontrolle

Wie unter 3.2.3 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit das Vorweisen und Überprüfen des digitalen Führerscheins im Zuge einer Verkehrskontrolle, wenn die Nutzer*in dies gegenüber dem Vorweisen des physischen Führerscheins bevorzugt. Der dabei zu erzeugende QR-Code, der hierzu eine Einsichtnahme in das FSR ermöglichen soll, enthält ua auch den MDS (Vorname, Nachname, Geburts-

datum). Dieser wäre zum Zweck des Abrufs der Ausweisdaten im FSR 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[148] und zum anderen, dem Organ im Falle einer mangelnden Internetverbindung Vorname, Nachname und Geburtsdatum der Person, die sich soeben im Zuge der Verkehrskontrolle mit dem digitalen Führerschein ausweist, wie beim Vorweisen eines physischen Ausweises unmittelbar ersichtlich zu machen.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Nach allen dem BMDW bzw BMF zum Zeitpunkt der Erstellung dieses Berichts vorliegenden Informationen ist eine Überprüfung des digitalen Führerscheins für Exekutivorgane ausschließlich im Rahmen der Verkehrskontrolle vorgesehen, zulässig und möglich.
- Für einen entsprechenden Zugriff auf das FSR ist eine Authentifizierung des jeweiligen Organs erforderlich und die entsprechende Serverkommunikation erfolgt verschlüsselt.
- Zuweisung von Rollen durch gesetzliche Bestimmungen bzw Auftragsverarbeitungsvereinbarungen

Ausweis offline vorweisen (außer Verkehrskontrolle)

Wie unter 3.2.4 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit das Vorweisen und Überprüfen des digitalen Führerscheins in allen anderen Fällen außer einer Verkehrskontrolle, wenn die Nutzer*in ihre Lenkberechtigung oder ihre Identität mit dem digitalen Führerschein nachweisen möchte.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Das Vorweisen des Ausweises findet offline statt (außer bei einer Verkehrskontrolle). Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.
- Die Daten, die die Nutzer*in des digitalen Führerscheins einer dritten Person, die ebenfalls die entsprechende Applikation nutzt, aus der Gesamtheit der im FSR gespeicherten Daten zur Verfügung stellen kann, hat der Gesetzgeber durch § 15a Abs 3 FSG auf jene beschränkt, die für den Nachweis der Lenkberechtigung erforderlich sind.
- Verschlüsselte Verbindung der dabei involvierten Endgeräte
- Nutzer*innen können selbst darüber entscheiden, wem sie ihren digitalen Führerschein vorweisen und daher mittelbar auch bis zu einem gewissen Grad, zu welchem Zweck diese Daten durch Dritte verarbeitet werden.

Widerruf des Gerätezertifikats AWP

Wie unter 3.2.5 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit, für den Fall, dass die ID Austria einer Person abläuft oder ungültig wird, auch die Anmeldung in der eAusweise-App dieser Person sowie die aktuell in die App geladenen Ausweise für ungültig zu erklären, da die eAusweise-App nur mit gültiger ID Austria verwendet werden kann.

[148] Im Einzelfall kann sich insbesondere der Nachname nach Ausstellung des Führerscheins geändert haben. Diese Änderung wäre nicht zwingend im FSR ersichtlich, jedoch im ZMR, aus welchem der MDS in der eAusweise-App letztlich im Wege der ID Austria stammt.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Der Personenbezug der Einträge in der Widerrufsliste kann nur in der AWP sowie durch die überprüfende App im Zuge der Überprüfung des Ausweises der jeweiligen betroffenen Person hergestellt werden und somit nur dann, wenn dies für den Zweck, dem die Widerrufsliste dient, erforderlich ist.
- Grundsätzlich rein automatisierte Verarbeitung, was einer zweckwidrigen Verarbeitung durch natürliche Personen vorbeugt

Abmelden von der eAusweise-App

Zweck dieser Verarbeitungstätigkeit ist, wie unter 3.2.6. erwähnt, das Löschen von Daten der Nutzer*in auf dem entsprechenden Endgerät bzw auf dem Server durch die betroffene Person selbst.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

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

Überprüfen des Ausweises in der eAusweise-App

Wie unter 3.2.7 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit die Verwendung der Funktion der eAusweise-App, einen Ausweis offline zu überprüfen, um so die Gültigkeit des digitalen Führerscheins einer anderen Person zu prüfen.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Vgl hierzu insb die Ausführungen iZm der initialen Anmeldung, zumal hierbei zunächst eine Authentifizierung der prüfenden Nutzer*innen erforderlich ist. Darüber hinaus 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 Ausweises (außer Verkehrskontrolle).

eAusweis Check-App

Wie unter 3.2.8 erwähnt, ist der Zweck dieser Verarbeitungstätigkeit die Verwendung der eigenständigen Überprüfungs-App, um die Gültigkeit des digitalen Führerscheins einer anderen Person zu prüfen.

Maßnahmen um zweckwidriger Verarbeitung entgegenzuwirken:

- Grundlegend werden hierbei keine personenbezogenen Daten der Nutzer*innen dieser Ausweis-Überprüfungs-App verarbeitet. Zur Verarbeitung personenbezogener Daten der *zu über-*

prüfenden Person siehe insbesondere die entsprechenden Ausführungen iZm dem Offline-Vorweisen des Ausweises (außer Verkehrskontrolle). Die Bereitstellung dieser Applikation stellt aber selbst eine Maßnahme dar, um die maximale informationelle Selbstbestimmung betroffener Personen zu verbessern, zumal diese demnach selbst entscheiden können, ob sie zur Prüfung von Ausweisen anderer Personen die eAusweise-App mit entsprechender Authentifizierung oder die anonyme eAusweis Check-App verwenden.

4.4.2 Grundsatz der Datenminimierung

Ein weiterer zentraler Grundsatz des Datenschutzrechts ist jener der Datenminimierung gem Art 5 Abs 1 lit c DSGVO. Die verarbeiteten personenbezogenen Daten sollten demnach für die Zwecke, zu denen sie verarbeitet werden, angemessen, erheblich und auf das für diese Zwecke notwendige Maß beschränkt sein.[149] 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 und damit auch dem Grundsatz der Datenminimierung; insbesondere werden die durch die betroffene Person auf eigene Initiative aus dem Führerscheinregister geladenen Ausweisdaten ausschließlich auf dem Endgerät der betroffenen Person gespeichert und das Vorweisen und Überprüfen des Ausweises erfolgt ausschließlich offline, dh ausschließlich auf den beiden verwendeten Endgeräten, und somit ohne dass dieser Vorgang eine Datenverarbeitung außerhalb der beiden verwendeten Endgeräte beinhaltet oder auslöst; zur Erforderlichkeit der davon abweichenden Implementierung der Verkehrskontrolle siehe am Ende dieses Abschnitts.
- Die Protokollierung ist hinsichtlich des Umfangs und der Speicherdauer auf das Minimum beschränkt; siehe dazu Abschnitt 4.6.7 unten.
- Daten werden gelöscht, wenn sie für ihren Zweck nicht mehr erforderlich sind; siehe dazu insbesondere auch Abschnitt 4.4.3 unten.
- Daten werden nur verarbeitet bzw übermittelt, soweit dies für den jeweiligen Zweck erforderlich ist; siehe dazu in Bezug auf die Verkehrskontrolle auch die Erwägungen am Ende dieses Abschnitts.

[149] Siehe auch ErwGr 39 DSGVO.

- Zugriffsrechte bestehen nur im erforderlichen Ausmaß.
- Es werden insb im Zuge der initialen Anmeldung keine zusätzlichen Daten bei der betroffenen Person erhoben, sondern das System setzt auf den bereits im Führerscheinregister vorhandenen Daten auf; der MDS der ID Austria ist hier insbesondere deswegen erforderlich, um der betroffenen Person im Falle eines Problems Support zu geben, da die betroffene Person ihr eigenes bPk prinzipienbedingt nicht kennt. Es steht eine eigene eAusweis Check-App zur Verfügung, die eine anonyme Überprüfung (ohne Anmeldung) ermöglicht.
- Die Aktualisierung von Ausweisdaten (sowohl zum Nachweis der Lenkberechtigung als auch iZm der Speicherung zum E-ID in vereinfachter Form) 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 der Verkehrskontrolle und des Offline-Vorweisens des Ausweises in allen anderen Fällen sind folgende Erwägungen in Hinblick auf die Erforderlichkeit und den Grundsatz der Datenminimierung zu erwähnen:

- Die zur Verkehrskontrolle befugten Organe haben bei der Verkehrskontrolle bereits bisher Zugriff auf das Führerscheinregister. Für den Anwendungsfall der Verkehrskontrolle wurde daher die Überprüfung des digitalen Führerscheins in § 15a Abs 1 FSG dem bisherigen Vorgehen bei Einsichtnahme in das Führerscheinregister nachgebildet, wobei im Fall des digitalen Führerscheins die Information, welcher Führerschein aus dem Führerscheinregister abzurufen ist, vom Endgerät der betroffenen Person mittels QR-Code zum Endgerät des überprüfenden Organs übertragen wird.
- Die zur Verkehrskontrolle befugten Organe benötigen auch deswegen im Zuge der Verkehrskontrolle unmittelbaren Zugriff auf das Führerscheinregister, um dort nötigenfalls die „Abnahme“ des digitalen Führerscheins vermerken zu können.[150]
- Mittels des QR-Codes wird im Rahmen der Verkehrskontrolle dem überprüfenden Organen auch der MDS übermittelt.[151] 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,[152] und zum anderen, dem Organ im Falle einer mangelnden Internetverbindung Vorname, Nachname und Geburtsdatum der Person, die sich soeben im Zuge der Verkehrskontrolle mit dem digitalen Führerschein ausweist, wie beim Vorweisen eines physischen Ausweises unmittelbar ersichtlich zu machen.

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.

[150] Dies kann dementsprechend auch nur durch authentifizierte Organe durchgeführt werden.
[151] Dies stellt eine minimalinvasive zusätzliche Verarbeitung dar, auch zumal diese Daten iaR ohnehin im Anschluss aus dem FSR geladen würden.
[152] Im Einzelfall kann sich insbesondere der Nachname nach Ausstellung des Führerscheins geändert haben. Diese Änderung wäre nicht zwingend im FSR ersichtlich, jedoch im ZMR, aus welchem der MDS in der eAusweise-App letztlich im Wege der ID Austria stammt.

Hierzu ist zunächst festzuhalten, dass Nutzer*innen die Löschung von Daten weitgehend selbst bestimmen, indem sie sich von der eAusweise-App abmelden (s dazu 3.2.6).

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

Einschlägige Informationen zur Speicherdauer von Daten finden sich in der Datenschutzinformation des *Verantwortlichen*.

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[153] präsentiert. Diese kann auch danach jederzeit auf der Startseite der App abgerufen werden.

Außerdem steht den Nutzer*innen im Zusammenhang mit der jedenfalls im Zuge des Registrierungsprozesses einmalig durchzuführenden Identitätsbestätigung der Zugriff auf die Datenschutzerklärung der dafür benötigten ID Austria mittels Link[154] 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[155] als auch auf der entsprechenden Website des BMF[156] 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.[157]

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

[153] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.
[154] Zum Zeitpunkt der Erstellung des Berichts unter https://www.oesterreich.gv.at/ueber-oesterreichgvat/datenschutz.html.
[155] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.
[156] Siehe https://www.bmf.gv.at/public/datenschutz.html.
[157] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.

Kontaktmöglichkeiten sind sowohl in der Datenschutzerklärung[158] als auch auf der entsprechenden Website des BMF[159] angegeben.

Ebenfalls kommt Betroffenen unter den in Art 17 DSGVO beschriebenen Voraussetzungen das Recht zu, vom *Verantwortlichen* die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Voraussetzungen sehen ein 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 Datenschutzerklärung[160] als auch auf der entsprechenden Website des BMF[161] 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[162] als auch auf der entsprechenden Website des BMF[163] 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.[164]

---

[158] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.
[159] Siehe https://www.bmf.gv.at/public/datenschutz.html.
[160] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.
[161] Siehe https://www.bmf.gv.at/public/datenschutz.html.
[162] Siehe https://www.oesterreich.gv.at/app-eAusweise/datenschutz.html bzw https://www.oesterreich.gv.at/app-eAusweise/datenschutz-digitaler-fuehrerschein.html.
[163] Siehe https://www.bmf.gv.at/public/datenschutz.html.
[164] 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.

4.6 Datenschutzrechtliche Anforderungen an die Protokollierung

Bevor im Rahmen dieses DSFA-Berichts auf die konkrete Ausgestaltung der Protokollierung mit Fokus auf die Risikoanalyse eingegangen wird, sollen im Folgenden die datenschutzrechtlichen Rahmenbedingungen[165] überblicksartig dargestellt werden.

Vorauszuschicken ist bereits an dieser Stelle, dass der Begriff der Protokollierung in der DSGVO nicht ausdrücklich genannt wird. Die Vornahme einer Protokollierung von Verarbeitungsvorgängen kann sich jedoch einerseits insb aus der Rechenschafts- und Nachweispflicht des *Verantwortlichen* (siehe Art 5 Abs 2 und Art 24 Abs 1 DSGVO),[166] andererseits auch aus Anforderungen an die Datensicherheit (Art 32 DSGVO)[167] ergeben. Daneben existiert in Bezug auf Einwilligungen gem Art 7 Abs 1 DSGVO eine spezifische Nachweispflicht, wonach der *Verantwortliche* die erfolgte Einwilligung der jeweils betroffenen Person nachweisen können muss, was ebenfalls im Ergebnis zu einer Protokollierung führen wird.[168]

Unmittelbar wird eine Protokollierung von Verarbeitungsvorgängen in § 50 DSG normiert, wobei diese Bestimmung in Umsetzung der JI-RL (EU) 2016/680 ergangen ist und daher nur einen (im vorliegenden Kontext nicht erfüllten) eingeschränkten Anwendungsbereich hat.[169]

Bei Protokolldaten handelt es sich nach der Entscheidungspraxis der Datenschutzbehörde idR um personenbezogene Daten.[170] Generell gilt es zu beachten, dass es durch die Vornahme einer Protokollierung auch zu einer eigenen Verarbeitung von Daten kommt,[171] welche (bei Vorliegen personenbezogener Daten) einer Rechtsgrundlage gem Art 6[172] bzw (bei Vorliegen „sensibler" Daten) Art 9 (jeweils iVm Art 5 bzw Art 32 DSGVO) bzw einer entsprechenden Norm im Unionsrecht oder dem nationalen Recht bedarf.

---

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

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

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

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

[169] § 50 DSG ist somit nur auf die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs anwendbar; auf die Protokollierung gem § 13 Abs 2 u 3 DSG wird an dieser Stelle mangels Relevanz nicht eingegangen.

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

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

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

Soweit die Aufzeichnung von Verarbeitungsvorgängen im Einzelfall nicht ausdrücklich gesetzlich angeordnet ist, wird sich die Zulässigkeit (bzw Unzulässigkeit) sowie in der Folge der Umfang der Durchführung einer Protokollierung aus einer **Gesamtbetrachtung** der Datenverarbeitung unter besonderer Beachtung des Grundsatzes der **Verhältnismäßigkeit** ergeben,[173] der sich (neben § 1 Abs 2 letzter Satz DSG)[174] auch in den datenschutzrechtlichen Prinzipien der Datenminimierung (Art 5 Abs 1 lit c DSGVO), der Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO) und der Integrität und Vertraulichkeit (Art 5 Abs 1 lit f DSGVO)[175] widerspiegelt. Der Grundsatz der Verhältnismäßigkeit erfordert, dass eine Verarbeitung personenbezogener Daten

- einem legitimen Zweck dient (siehe dazu unter 4.6.3),
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen, und
- angemessen, dh verhältnismäßig im engeren Sinne, ist.[176]

Der Grundsatz der Erforderlichkeit besagt, dass eine Verarbeitung personenbezogener Daten nur so weit zulässig ist, als dies für die Erreichung des damit verfolgten Zwecks notwendig ist,[177] es also kein milderes, gleich effektives Mittel gibt. Im Rahmen von Protokollierungsvorgängen wird die Erforderlichkeit einer Protokollierung (und deren Umfang) insb anhand des konkreten **Verarbeitungskontextes**, des **Schutzbedarfs** und der **Risikobewertung** zu beurteilen sein.

In diesem Zusammenhang ist auch Art 5 Abs 1 lit c DSGVO relevant, der die Verarbeitung personenbezogener Daten von der Einhaltung des Grundsatzes der **Datenminimierung** abhängig macht. Laut EuGH geht aus dem Wortlaut dieser Bestimmung hervor, dass mit diesem Prinzip kein allgemeines und absolutes Verbot [der Datenverarbeitung] eingeführt werden soll.[178] Daraus ergibt sich in einer **Gesamtbetrachtung** bei der Speicherung von Protokolldaten also kein Verbot, sondern eine Prüfung auf die Einhaltung des Verhältnismäßigkeitsgrundsatzes im Einzelfall und insbesondere der konkret erforderlichen Datenfelder für die Zweckerreichung der Protokollierung.

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

4.6.1 Was versteht man unter „Protokollierung“?

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

---

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

wie zB Speicherung, Veränderung, Abfragen, Abgleichen, Löschen)[179] zusammen mit weiteren Metadaten, wie Datum und Zeit des jeweiligen Vorganges („Timestamp"), aufgezeichnet. Ergebnis der Speicherung dieser Protokolldaten sind sogenannte „Protokolle" – auch „Logfiles" oder „Protokolldateien" genannt. Laut dem deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) kann grundsätzlich zwischen zwei Protokollierungsebenen unterschieden werden:[180]

- Protokollierung technischer Systemereignisse auf **Ebene der IT-Infrastruktur („Infrastrukturebene")** zum Zweck der Überwachung der IT-Sicherheit bzw der Datensicherheit[181] (zB Erkennung unbefugter Aktivitäten) sowie der Sicherstellung der ordnungsgemäßen Funktion bzw der Verifizierung und Behebung von Systemfehlern;[182]
- datenschutzrechtlich normierte Protokollierung auf **fachlicher Ebene („Anwendungsebene").**[183] Sie dient insbesondere dem Ziel, eine effiziente Nachprüfbarkeit einzelner Verarbeitungsvorgänge zu ermöglichen, worunter auch die Eigenkontrolle fällt.[184] Zu den protokollierten Vorgängen zählen – abhängig von der konkreten Ausgestaltung – insbesondere Aktivitäten der Nutzer*innen („User") der Anwendungen, wozu sowohl Administrator*innen als auch Endnutzer*innen zählen.

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

4.6.2 Inhalt von Protokolldaten

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

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

onssicherheitshandbuch dazu ausgeführt, dass *„Art und Umfang von Protokollierungen von den speziellen Anforderungen des IT-Systems und der darauf befindlichen Applikationen und Daten ab[hängen] und im Einzelfall sorgfältig festzulegen [sind].“*[185]

Beispielhaft muss bei Vorliegen des Protokollierungszwecks „Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ aus **datenschutzrechtlicher** Sicht anhand der Logdateien verifiziert werden können, **wer wann welche** personenbezogenen Daten **wie** verarbeitet hat. So wird im deutschen Standarddatenschutzmodell (SDM) gefordert, dass zur vollständigen Prüfung zumindest die folgenden Protokolldaten erforderlich sind:[186]

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

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

4.6.3 Wozu wird protokolliert?

Als üblicher Zweck der Protokollierung (aus Sicht des Datenschutzrechts und insbesondere der Datensicherheit) ist vor allem die Nachprüfbarkeit der datenschutzrechtlich relevanten Vorgänge anzuführen. Diese Nachprüfbarkeit einzelner Verarbeitungsvorgänge ist dabei Grundvoraussetzung für die Erbringung eines Nachweises der Einhaltung der rechtlichen Datenschutzanforderungen durch den *Verantwortlichen* (Rechenschaftspflicht gem Art 5 Abs 2 DSGVO).[187] Die Kontrollierbarkeit der Ordnungsmäßigkeit der Datenverarbeitung durch Protokollierung ist gleichzeitig auch eine Maßnahme zur Sicherstellung von Informations- und Datensicherheit.[188]

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

Der Zweck der Protokollierung besteht aber auch darin, eine Verarbeitung personenbezogener Daten transparent zu gestalten, betroffenen Personen über die Verarbeitung ihrer Daten auf Nachfrage eine Auskunft erteilen zu können.[189]

---

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

4.6.4 Auswertung von Protokollen

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

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

Mit Bezug auf § 18 Abs 1 letzter Satz E-GovG – wenn auch hier nicht unmittelbar einschlägig – kann aus dem Gesetzeswortlaut und den Materialien[190] abgeleitet werden, dass es dem *Verantwortlichen* und dem *Auftragsverarbeiter* nicht verwehrt ist, den Grundsätzen für die Verarbeitung personenbezogener Daten nachzukommen, worunter zB im Rahmen der Überprüfung der Rechtmäßigkeit der Datenverarbeitung auch die (interne) Auswertung von Protokolldaten fallen wird. Dabei ist jedoch darauf zu achten, dass dabei nur die im Einzelfall relevanten (personenbezogenen) Daten ausgewertet werden dürfen.

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

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

2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet."[191]

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

[190] ErläutRV 469 BlgNR 27. GP 7.

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

Gewährleistung der Revisionssicherheit der Protokolldaten (Manipulationsschutz).[192] Kurz gesprochen: Je höher das (potenzielle) Risiko der Verarbeitung für die betroffenen Personen ist, desto umfangreicher muss der Schutz der Protokolldaten ausfallen.

4.6.5 Wie lange dürfen Protokolle aufbewahrt werden?

Konkrete Aufbewahrungsfristen für Protokolldaten finden sich weder in der DSGVO noch im geltenden DSG. Bis zum Ablauf des 24. 5. 2018 waren gem § 14 Abs 5 DSG 2000 Protokoll- und Dokumentationsdaten grds drei Jahre lang aufzubewahren, sofern gesetzlich nicht ausdrücklich anderes angeordnet war.

Mangels ausdrücklicher Anordnung der Speicherdauer durch eine Rechtsnorm (welche aus grundrechtlicher Sicht selbstverständlich in verhältnismäßiger Weise ausgestaltet sein muss) ergibt sich die Aufbewahrungsdauer aus dem Vorliegen der Erforderlichkeit für den jeweiligen Auswertungszweck. Wie lange dieses Kriterium der Erforderlichkeit vorliegt, ist häufig das Ergebnis einer Abwägung, in die neben dem Zweck auch Art und Inhalt der protokollierten Ereignisse und das Ergebnis einer Risikobewertung einfließen können.[193]

In diesem Sinne hat der Gesetzgeber in den Materialien zur Protokollierung gem § 50 DSG nachvollziehbar (und uE verallgemeinerungsfähig) erläutert, dass *„[…] Protokolldaten – wie auch alle anderen personenbezogenen Daten – nur solange in personenbezogener Form aufbewahrt werden [sollten], als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; danach sind die Protokolldaten zu löschen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen. Eine längere Aufbewahrungsdauer muss sich aus besonderen gesetzlichen Vorschriften ergeben.“*[194]

Zumindest personenbezogene Teile von Protokolldaten sind daher nach Zweckerreichung zu löschen bzw zu anonymisieren,[195] sofern auch keine sonstigen gesetzlichen Aufbewahrungsfristen mehr bestehen. In jenen Fällen, in denen die Protokolldaten auch Inhaltsdaten enthalten, darf die Aufbewahrung der Protokolldaten nicht zu einer Umgehung der Löschungsverpflichtung des originären Inhaltsdatums führen.[196]

Interessant sind die (allerdings im Rahmen eines Art 36 DSGVO-Verfahrens im Bereich einer deutschen Rundfunkanstalt ergangenen) Ausführungen zur Speicherdauer von Logdaten zur Feststellung bzw Abwehr von Cyberattacken.[197] Obwohl deutsche Rundfunkanstalten (jedenfalls zum Zeitpunkt der Entscheidungsfindung) nicht als Betreiber einer kritischen Infrastruktur zu qualifizieren waren, verwies

---

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

der Rundfunkdatenschutzbeauftragte auf die Empfehlung des BSI an Betreiber kritischer Infrastrukturen iSd deutschen BSI-Gesetzes, welche die Speicherung von Logdaten, jedenfalls für Proxy- und Firewall-Logs, für die Dauer von mindestens 90 Tagen vorsieht.[198] Bei zu erwartenden Beschwerden an die Datenschutzbehörde wäre auch die Heranziehung der Fristen in § 24 Abs 4 DSG denkbar. Für die kommende eIDAS 2-VO schlägt ein renommierter Experte eine Aufbewahrungsdauer zwischen zwei Jahren und einem Monat vor, welche aufgrund einer durchgeführten DSFA festzulegen sei.[199]

Das Ergebnis hinsichtlich der Speicherdauer von Protokolldaten muss uE – nicht zuletzt für die interne Umsetzung der Protokollierung und die (externe) Vorlage in einem etwaigen Verfahren vor der Datenschutzbehörde bzw vor Gericht – durch den *Verantwortlichen* niedergeschrieben, also dokumentiert werden. Hierfür ist die Erstellung eines sogenannten Protokollierungskonzepts empfehlenswert.[200]

4.6.6 Exkurs: Auskunftsrecht der betroffenen Personen

Teil der Betroffenenrechte ist das in Art 15 DSGVO normierte Recht auf Auskunft darüber, ob über die (anfragende) betroffene Person personenbezogene Daten verarbeitet werden. Da das Auskunftsrecht (bis auf Rechte und Freiheiten anderer Personen, siehe Art 15 Abs 4 leg cit; beachte auch § 4 Abs 5 und 6 DSG zur Gefährdung gesetzlich übertragener Aufgaben bzw von Geschäfts- oder Betriebsgeheimnissen) nicht weiter eingeschränkt wird, werden davon grds auch (personenbezogene) Protokolldaten erfasst sein, da der EuGH in seiner bisherigen Rsp dieses Betroffenenrecht tendenziell weit ausgelegt hat.[201] Dass jedoch noch Unklarheiten bei der Auslegung der DSGVO bestehen, die auch Art 15 betreffen, zeigt das rezente Vorabentscheidungsverfahren vor dem EuGH, worin auch das Auskunftsrecht über Protokolldaten thematisiert wird.[202]

Eine Umgehung des (verfassungsrechtlich in § 1 Abs 3 Z 1 DSG und Art 8 Abs 2 GRC festgeschriebenen) Auskunftsrechts durch fehlendes Anlegen von Protokollen, wo dieses gem Art 5 Abs 2 oder Art 32 DSGVO oder sonstige Rechtsgrundlagen erforderlich ist, ist wohl nicht rechtskonform. So hat die DSB auf Grundlage von Art 5 Abs 2 DSGVO entschieden, dass sich ein *Verantwortlicher* der Einhaltung seiner durch die DSGVO auferlegten Pflichten nicht dadurch entziehen kann, indem er ungeeignete technische und organisatorische Maßnahmen trifft, die es ihm ua verunmöglichen, den Anträgen von betroffenen Personen zu entsprechen.[203]

---

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

[199] *Olejnik*, Privacy analysis of European eID Regulation proposal (Pkt 13), https://blog.lukaszolejnik.com/privacy-analysis-of-european-eid-regulation-proposal/ (zuletzt abgerufen am 2. 3. 2022): "In Article 6a(7): "*The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services."* It should also be defined that the collected information is deleted when not needed: after a time as defined in the DPIA documents prepared. Such a time period may be stipulated in the Regulation itself. It should not exceed two years, possibly even a month?"

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

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

[202] Anhängig unter C-579/21.

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

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

4.6.7. Umsetzungsstrategie zur Protokollierung im Rahmen der Ausweisplattform

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

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

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

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

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

Auch Vorgänge des Vorweisens und Überprüfen von Ausweisen werden im System der Ausweisplattform nicht protokolliert. Dies gilt sowohl beim Ausweis offline Vorweisen als auch bei der Verkehrskontrolle.[204]

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

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

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

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

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

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

Initiale Anmeldung an der eAusweise-App und Einrichtung

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

Führerschein laden

Die wesentliche Information über erfolgte Verarbeitungsvorgänge, nämlich ob eine bestimmte betroffene Person ihren Führerschein auf ihr Endgerät geladen hat, ergibt sich hierbei aus dem jeweiligen Eintrag, der in diesem Fall in der Ausweisplattform vorhanden sind. Zu beachten ist zudem in diesem Zusammenhang, dass gemäß § 16b Abs 7 FSG aufseiten des Führerscheinregisters – und somit außerhalb der Systemgrenzen der Ausweisplattform und der Zuständigkeit von dessen Verantwortlichen –

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

eine vollständige Protokollierung aller erfolgten und versuchten Datenabfragen und somit auch von Datenabfragen im Zuge von Verkehrskontrollen, durchgeführt wird, aus der erkennbar ist, welcher Person welche Daten aus dem Führerscheinregister übermittelt wurden, wobei die Protokolldaten für drei Jahre aufbewahrt werden.

Verkehrskontrolle

Das Vorweisen bzw Überprüfen des digitalen Führerscheins im Zuge einer Verkehrskontrolle wird im System der Ausweisplattform nicht protokolliert. Zu beachten ist jedoch, dass gemäß § 16b Abs 7 FSG aufseiten des Führerscheinregisters – und somit außerhalb der Systemgrenzen der Ausweisplattform und der Zuständigkeit von dessen Verantwortlichen – eine vollständige Protokollierung aller erfolgten und versuchten Datenabfragen und somit auch von Datenabfragen im Zuge von Verkehrskontrollen, durchgeführt wird, aus der erkennbar ist, welcher Person welche Daten aus dem Führerscheinregister übermittelt wurden, wobei die Protokolldaten für drei Jahre aufbewahrt werden.

Ausweis offline vorweisen (außer Verkehrskontrolle)

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

Widerruf des Gerätezertifikats AWP

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

Abmelden von der eAusweise-App

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

Überprüfen des Ausweises in der eAusweise-App

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

eAusweis Check App

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

4.7 Datenübermittlung in Drittländer (oder an internationale Organisationen)

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

4.8 Rat des Datenschutzbeauftragten und Standpunkt der Betroffenen

Nach Art 35 Abs 2 DSGVO hat der Verantwortliche bei Durchführung einer DSFA den Rat des Datenschutzbeauftragten einzuholen. Ob der Rat des Datenschutzbeauftragten verpflichtend einzuholen ist und inwiefern dem eingeholten Rat des Datenschutzbeauftragten zu folgen ist, wird in der Literatur uneinheitlich kommentiert: *Trieb* geht bspw davon aus, dass die DSGVO keine solche Pflicht statuiert;[205] *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.[206] Falls der Verantwortliche mit dem vom Datenschutzbeauftragten eingeholten Rat (oder Teilen davon) nicht einverstanden ist, sollte nach Ansicht der Art-29-Datenschutzgruppe jedoch eine (nachvollziehbare) Begründung für die mangelnde Beachtung des Ratschlags in den DSFA-Bericht aufgenommen werden.[207]

Im vorliegenden Fall wurde die Konsultation der Datenschutzbeauftragten des BMDW an der bewährten und mit diesen auch akkordierten Vorgehensweise bei der Erstellung des DSFA-Berichts für die ID Austria orientiert. Der bereits in der Einleitung beschriebene Wechsel der Ressortzuständigkeit, der effektiv am 18. Juli 2022 nach Inkrafttreten der Novelle zum Bundesministeriengesetz erfolgte, brachte es mit sich, dass ab diesem Zeitpunkt die Möglichkeit der Einbindung des Datenschutzbeauftragten des BMF bestand und umgehend genützt wurde.

Ferner ist vom Verantwortlichen gemäß Art 35 Abs 9 DSGVO im Zuge einer DSFA gegebenenfalls der Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen.[208] Die Bestimmung des Abs 9 schafft grundsätzlich die Möglichkeit, die individuelle Meinung einzelner Betroffener in Erfahrung zu bringen.[209] Alternativ können auch deren "*Vertreter*" herangezogen werden, wobei in erster Linie an verschiedene Interessensvertretungen, Betriebsräte oder Verbraucherschutzverbände zu denken ist; der Standpunkt dieser Einrichtungen sollten insb dann berücksichtigt werden, wenn die beabsichtigte Datenverarbeitung eine große Zahl betroffener Personen erfasst, deren Interessen der jeweilige Verband oder die jeweilige Stellte vertritt.[210] Auch diese Regelung lässt in mehrfacher Hinsicht Deutungsspielräume offen.[211] 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.[212] Eine bedingungslose Verpflichtung für Verantwortliche zur Einholung wird auf Basis dieser Bestimmung

[205] Vgl *Trieb*, in *Knyrim*, DatKomm Art 35 Rz 124.
[206] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 18.
[207] So die *Art-29-Datenschutzgruppe*, WP 243 rev. 01, 17 unter Hinweis auf Art 24 Abs 1 DSGVO.
[208] 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.
[209] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.
[210] 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.
[211] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff.
[212] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 54 ff; In der englischen Version der DSGVO wird bspw die Formulierung „where appropriate" verwendet; vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 131.

nicht unterstellt werden können;[213] die jeweilige Vorgehensweise ist jedoch zu dokumentieren bzw zu begründen.[214]

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

[213] Vgl *Trieb* in *Knyrim*, DatKomm Art 35 Rz 131.
[214] Vgl *Jandt*, in *Kühling/Buchner* DS-GVO/BDSG Art 35 Rz 58.

5 Datenschutzrechtliche Risikoabschätzung – Risk Assessment

Aus Art 35 Abs 7 lit c DSGVO ergibt sich für die ordnungsgemäße Durchführung einer DSFA die rechtliche Anforderung zur "Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen". Während die Formulierung "Rechte und Freiheiten natürlicher Personen" primär auf die Ziele der DSGVO gem Art 1 Abs 2 referenziert,[215] 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.[216] 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.[217] Dabei werden exemplarisch die folgenden Szenarien angeführt:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzieller Verlust,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- unbefugte Aufhebung der Pseudonymisierung.

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

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

---

[215] 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.

[216] 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.

[217] Vgl ErwGr 75 DSGVO. Siehe auch *Martin et al*, Datenschutz-Folgenabschätzung 39 f; zur methodischen Konkretisierung der Begriff "Eintrittswahrscheinlichkeit" und "Schwere" siehe Kapitel 5.1.

Weitere exemplarisch angeführte Bedrohungsszenarien für den Bereich der IT-Sicherheit können ua den IT-Grundschutz-Katalogen des deutschen Bundesamts für Sicherheit in der Informationstechnik entnommen werden.[218]

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

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

Sollten sich die Datenverarbeitungsprozesse oder das Risikoumfeld ändern, ist jedenfalls zu überprüfen, ob die DSFA noch der Realität entspricht und bei Bedarf eine Aktualisierung vorzunehmen.[219]

[218] https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf.
[219] 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.[220] Darüber hinaus wurde Anleihe am Risk Assessment-Leitfaden des deutschen Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom),[221] sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Fraunhofer-Institutes für System- und Innovationsforschung genommen.[222]

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.[223]

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[224]

- 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.[225]

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.[226]

In den methodischen Ausführungen des Fraunhofer-Instituts werden für die generelle Erfassung eines Risikoszenarios wiederum die folgenden übergeordneten Fragen aufgeworfen:[227]

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

---

[220] https://www.iso.org/standard/65694.html.
[221] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung, https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf (2017).
[222] 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.
[223] Vgl *European Data Protection Supervisor (EDPS)*, Accountability on the ground Part II: Data protection Impact Assessments & Prior Consultation (2019) 6.
[224] 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.
[225] Siehe Art 35 Abs 7 lit d sowie ErwGr 84 und 90 DSGVO.
[226] Vgl ErwGr 83 DSGVO.
[227] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 43.

– Welche Abhilfemaßnahmen sind bereits implementiert bzw geplant?[228]

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:[229]

– **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“*.[230]

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

[228] Zudem kann ergänzt werden, welche zusätzlichen Maßnahmen sich bestimmen lassen um die identifizierten Risiken zu mitigieren.
[229] 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.
[230] Vgl ErwGr 76 DSGVO.

Risikobeurteilung (Template)

1) Risikoidentifikation	**Risikobeschreibung**
	Beschreibung und kurze deskriptive Erläuterung des Szenarios, Nennung beteiligter Akteure und Personen,[231] Nennung verarbeiteter Datenkategorien
	Risikoquelle
	Was sind die auslösenden Elemente für den Schadenseintritt? **Handelt es sich um eine menschliche oder technische Risikoquelle?** **Interne menschliche Quellen:** Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar **Externe menschliche Quellen:** Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler Vorsätzliches Handeln: Angreifer oder Verursacher außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Systems oder der Betroffenen **Interne / externe technische Quellen:** Systemfehler (Software/Hardware) führen zu Verlust, Veränderung; Nichtverfügbarkeit oder missbräuchlicher Verwendung personenbezogener Daten **Bsp Risikoquelle:** • Interne Mitarbeiter*innen, • Externe Mitarbeiter*innen, • Betroffene, • Sonstige Dritte, • Softwarefehler, • Hardwaredefekt (physikalisch), • Umwelteinflüsse (Naturgewalt), • Cyberkriminelle (Hacker/Schadsoftware), • staatliche Institutionen (Nachrichtendienste, Strafverfolgung), • Geschäftsführung.
	Risikoursache
	Was löst den Eintritt des Schadens aus und führt zur „Verwirklichung des Risikos“? Dies dürfte regelmäßig in der Nichteinhaltung der Datenschutzgrundsätze (Art 5 Abs 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art 12 bis 22 DSGVO) oder

[231] Siehe hierzu auch die Auflistung an zu prüfenden Organisationen bei *Friedewald/Bieker/Obersteller/Nebel/Martin/Rost/Hansen* Datenschutz-Folgenabschätzung (2017), *https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf (abgerufen am 24. 8. 2022)* 30 f.

	anderer Verstöße gegen die DSGVO (wie zB einem ungerechtfertigten Datentransfer ins Ausland) liegen.[232] **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?[233] **Bsp physische Schäden:** körperliche Schäden (zB durch falsche medizinische Behandlung); wenn Verstöße gegen die Vertraulichkeit Gewaltverbrechen, einschließlich Stalking, Vorschub leisten; psychologische Schäden (wie zB Angstzustände oder Depressionen) **Bsp materielle Schäden:** wirtschaftliche Schäden, berufliche Nachteile (wie zB entgangene Einstellung oder Beförderung, Jobverlust), Beschneidung staatlicher Leistungen (wie zB Arbeitslosengeld, Sozialhilfe), Diskriminierung (zB bei Versicherungsabschlüssen oder Wohnungssuche), ungerechtfertigte Gebühren oder Bußgelder usw **Bsp immaterielle Schäden:** gesellschaftliche und soziale Nachteile (wie etwa Rufschädigung oder Verleumdung, Mobbing, Diskriminierung usw); Schädigung der Privatsphäre (wie etwa das Gefühl, aufgrund von biometrischer Erkennung, oder Tracking über Webseiten, Applikationen und Endgeräte hinweg, ausgespäht zu werden); Einschüchterungseffekte (sog „chilling effects“, wenn Menschen aus Angst davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit auszuleben bzw zu entfalten); ungerechtfertigte Beeinträchtigung von Rechten (durch Verarbeitung ohne ausreichende Rechtsgrundlage)

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

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

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

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

Der Prozess der datenschutzrechtlichen Risikobeurteilung erfolgt im vorliegenden Fall somit anhand der folgenden fünf Teilschritte: Risikoidentifikation; Risikoanalyse und -bewertung; Ermittlung bestehender Maßnahmen und Festlegung zusätzlicher Maßnahmen der Risikomitigierung und schließlich die neuerliche Risikoanalyse und -bewertung unter Berücksichtigung der zum Zeitpunkt der Beurteilung tatsächlich vorgesehenen Abhilfemaßnahmen. Die zuvor dargelegte Sachverhaltsbeschreibung dient als Informationsgrundlage der Risikobeurteilung.[234] Die Risikoidentifikation bezieht sich auf diese Grundlage und extrahiert daraus für die weitere Risikoanalyse wesentliche datenschutzrechtliche Aspekte wie die Nennung der involvierten Akteure bzw Personen, die Beschreibung der Risikoursache bzw -quelle, sowie die Bestimmung möglicher physischer, materieller oder immaterieller Schäden.

Die anschließende Risikoanalyse und -bewertung stellt aus methodischer Sicht einen Prozess der Quantifizierung des vorab geschilderten und identifizierten Risikoszenarios dar. Dabei werden Eintrittswahrscheinlichkeit und Schwere des Risikos jeweils anhand der Skalen-Ausprägung „vernachlässigbar", „eingeschränkt", „wesentlich" bzw „maximal" eingestuft.[235] Im Zuge der Risikobeurteilung sind

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

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

die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu eruieren.[236] Tabelle 1 und 2 zeigen die hinter den rangskalierten Merkmalsausprägungen stehenden Annahmen zur angemessenen Einstufung des identifizierten Risikoszenarios.[237]

Tabelle 1: Risikoausprägung für Eintrittswahrscheinlichkeit[238]

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[239]

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

Nach Analyse und Zuordnung werden die jeweiligen Skalenwerte in einer Risikomatrix verortet. Der Risikograd ist methodisch definiert als das Produkt von Eintrittswahrscheinlichkeit und Schadensausmaß.[240] 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,[241] wie in der nachfolgenden Risikomatrix dargestellt.

[236] Vgl ErwGr 75 und 76 DSGVO.
[237] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 ff; vgl *CNIL*, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases) (2015) 13 ff.
[238] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 30 f.
[239] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 50 f.
[240] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 8 (9).
[241] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46; vgl hierzu weiterführend auch *Friedewald et al*, Datenschutz-Folgenabschätzung 31.

Tabelle 3: Risikomatrix

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

Um der grundrechtlichen Schutzkonzeption des Datenschutzrechts gerecht zu werden, wird im Schrifttum jedoch auch empfohlen, dass die Beurteilung eines Risikos nicht ausschließlich anhand der quantitativen Matrix von Schadenshöhen (Schwere) und Eintrittswahrscheinlichkeiten bestimmt werden sollte. Vielmehr ist davon auszugehen, dass generell jede Datenverarbeitung einen Eingriff in die Grundrechte der Betroffenen gem Art 7 und 8 der GRC darstellt und sich auch aus einer völlig rechtskonformen Datenverarbeitung bereits ein "normaler" Schutzbedarf ergibt.[242]

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.[243] Dabei werden bestehende technische und organisatorische Maßnahmen zur Behandlung des Risikos ermittelt und aufgezeigt. Die Maßnahmen können die Gestaltung und Entwicklung des Systems ebenso betreffen, wie den operativen Betrieb. Im Zuge dessen ist insb den Grundsätzen des Datenschutzes durch Technikgestaltung (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) Genüge zu tun.[244]

Die in Art 35 Abs 7 lit d DSGVO genannte „Bewältigung" wird gemeinhin auch als „Reduktion" bzw „Eindämmung" verstanden.[245] Durch die Maßnahmen sollten zumindest alle als „hoch" bewerteten Risiken so weit reduziert werden, dass sie nur noch als „normal" einzustufen sind.[246] Dabei ist es nicht zwangsläufig notwendig, zusätzliche Maßnahmen zu implementieren; mitunter kann es auch sinnvoller sein, bestehende Maßnahmen zu stärken.[247]

[242] Vgl *Friedewald et al*, Datenschutz-Folgenabschätzung 31.
[243] Siehe Art 35 Abs 7 lit d DSGVO; vgl *Martin et al*, Datenschutz-Folgenabschätzung 38.
[244] Vgl ErwGr 78 DSGVO.
[245] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 46.
[246] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 47.
[247] Vgl *Martin et al*, Datenschutz-Folgenabschätzung 48.

In Art 32 Abs 1 DSGVO werden zur Gewährleistung eines angemessenen Schutzniveaus folgende Optionen bzw Maßnahmen der Risikobehandlung angeführt:[248]

- 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.[249] Die verschiedenen Maßnahmen, Garantien und Verfahren sollen letztlich den Schutz personenbezogener Daten sicherstellen und die Einhaltung der Bestimmungen dieser Verordnung nachweisen.[250]

Nach Ermittlung und Bestimmung der Maßnahmen wird im vorliegenden Modell der Risikobeurteilung der Schritt zur Risikoanalyse und -bewertung wiederholt und eine neuerliche Klassifizierung und Errechnung des Risikograds vorgenommen. Über diesen zweiten Analyse- bzw Bewertungsschritt wird der potenzielle Einfluss der vorab festgelegten Maßnahmen der Risikomitigierung verdeutlicht.

Abschließend geht es in einer generellen Zusammenschau um die Feststellung des verbleibenden Restrisikos und der damit verbundenen weiteren Risikobehandlung durch den *Verantwortlichen*.[251] 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.[252] 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.[253]

---

[248] Vgl *Bitkom*, Risk Assessment & Datenschutz-Folgenabschätzung (2017) 33 f.
[249] 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.
[250] Vgl ErwGr 90 DSGVO.
[251] 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.
[252] 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.
[253] 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.[254] 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 der eAusweise-App und des digitalen Führerscheins

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person lehnt zwar digitale Ausweise generell ab und möchte daher weder den digitalen Führerschein noch die eAusweise-App nutzen, installiert und verwendet diese aber dennoch, weil sie entweder durch äußere Umstände einem Druck ausgesetzt ist, dies zu tun oder der (irrigen) Annahme unterliegt, künftig bei Verkehrskontrollen den Führerschein in digitaler Form vorweisen zu müssen. Insbesondere falls die Nutzung des digitalen Führerscheins künftig weite Verbreitung finden sollte, kann es zu Formen sozialen Drucks oder faktischen Zwangs zur Nutzung des digitalen Führerscheins als Identitätsnachweis 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. In Fällen, in denen bisher eine anonyme bzw pseudonyme Nutzung möglich war, kann es dazu kommen, dass von privater Seite die Identifikation mittels staatlich geprüfter Identität verlangt wird, weil dies durch den digitalen Führerschein erleichtert wird. 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

[254] 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 der analoge Führerschein weiterhin uneingeschränkt genutzt werden kann • Größere Zahl von Privaten, insbesondere Unternehmen, deren Verhalten zu entsprechenden Drucksituationen führt • 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 Führerscheins 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) Kommentar: Wenn sich dieses Risiko materialisiert, wird die betroffene Person unfreiwillig dem Potenzial ausgesetzt,	Hoch (12)

		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 des physischen Führerscheins • Das Datenschutzrecht untersagt das Verlangen der Identität oder 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 Ausweises oder derzeit konkret des digitalen Führerscheins als einzig zulässige Variante für die Bürger*in festlegt, noch ist nach derzeitigem Wissensstand ein solcher angedacht oder gar in Planung. In der Außenkommunikation wird das BMF deutlich auf diesen Umstand hinweisen.

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

5.2.2 Diskriminierung aufgrund von Nicht-Nutzung der eAusweise-App

1) Risikoidentifikation	**Risikobeschreibung**
	Die betroffene Person verwendet die eAusweise-App bzw den digitalen Führerschein 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 Führerscheins könnte es uU zu Situationen kommen, in denen insb private *Verantwortliche* auf das Vorweisen eines digitalen Ausweises bestehen, insb weil im Vergleich dazu das Auslesen für die überprüfende Person leichter und die Fälschungssicherheit höher ist. Dadurch würden potenziell Personen diskriminiert, die keine eAusweise-App oder keinen digitalen Führerschein 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 Führerscheins. • Einschränkung der informationellen Selbstbestimmung • Verhalten privater Anbieter (zB Autovermietungen), 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 der physische Führerschein weiterhin uneingeschränkt genutzt werden kann
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden:

	• Möglicher Ausschluss von system- oder alltagsrelevanten Diensten, womit auch finanzielle Schäden verbunden sein könnten (zB höherer Mietwagenpreis, weil ein günstigerer Anbieter den digitalen Führerschein 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 Führerschein 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. • Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Führerscheins als moderne Inklusionsvariante einen erleichterten Zugang zu einem Verwaltungsprozess darstellt und somit gleichsam als Gegenteil eines Diskriminierungsinstruments konzipiert ist

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

5.2.3 Unfreiwillige Nutzung biometrischer Authentifizierungsfunktionen

1) Risikoidentifikation	**Risikobeschreibung**
	Die eAusweise-App setzt zwingend das Vorhandensein und die Verwendung einer biometrischen Authentifizierungsfunktion auf dem Endgerät der betroffenen Person voraus (Fingerabdruck-Sensor oder Face ID). Das bedeutet, auf dem Endgerät der betroffenen Person werden zum Zweck der Authentifizierung biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) und somit sensible Daten iSv Art 9 Abs 1 DSGVO verarbeitet.[255] Insbesondere falls die Nutzung des digitalen Führerscheins künftig weite Verbreitung finden sollte, kann es zu Formen sozialen Drucks oder faktischen Zwangs zur Nutzung der eAusweise-App bzw des digitalen Führerscheins kommen. Personen, die die Verwendung biometrischer Daten zu Authentifizierungszwecken auf ihrem mobilen Endgerät ablehnen, könnten auf diese Weise in die Situation kommen, dass sie die biometrischen Authentifizierungsfunktionen gegen ihren Willen trotzdem nutzen, um die eAusweise-App verwenden zu können und dadurch Nachteile zu vermeiden. Dieses Risiko kann auch ohne eAusweise-App eintreten, aber die eAusweise-App kann sich diesbezüglich risikoerhöhend auswirken, nämlich dann, wenn die betroffene Person nur deswegen begonnen hat, die Biometriefunktion des Endgeräts zu nutzen, um die eAusweise-App zu nutzen. Für diese Personen bewirkt die eAusweise-App, dass überhaupt erst ein Risiko für ihre biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art 4 Z 14 DSGVO) entsteht.
	Risikoquelle
	Externe menschliche Quelle: • Sonstige Dritte (insb Anbieter*innen von Drittdiensten) **Interne technische Quelle:** • Softwarearchitektur (Mangel an alternativen Authentifizierungsformen)
	Risikoursache
	• Marktdynamiken in gewissen Bereichen aufgrund von voranschreitender Digitalisierung führen zu entsprechendem Druck zur Nutzung der eAusweise-App. • Heranziehen von Biometrie zur Authentifizierung • Einschränkung der informationellen Selbstbestimmung
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden

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

	• Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung von Biometrie verbunden sind, da die betroffene Person diese eigentlich gar nicht verwenden würde, wenn sie sich frei entscheiden hätte können **Immaterielle Schäden:** • Verarbeitung personenbezogener Daten gegen den Willen der betroffenen Person • Aufgrund einer eingeschränkten, mangelhaften bzw fehlenden Freiwilligkeit der Einwilligung kommt es zu einer unrechtmäßigen Datenverarbeitung. • Eröffnung des Potenzials, dass sich eines der anderen nachfolgend beschriebenen Risiken materialisiert, die mit der Verwendung von Biometrie verbunden sind, da die betroffene Person diese eigentlich gar nicht verwenden würde, wenn sie sich frei entscheiden hätte können

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Maximal (4)	Wesentlich (3) Kommentar: Wenn sich dieses Risiko materialisiert, wird die betroffene Person unfreiwillig dem Potenzial ausgesetzt, dass sich das biometriebezogene Risiko 5.2.10 materialisiert.	Hoch (12)

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

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

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.[256] 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 – von gewissen Altersgruppen abgesehen – 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 • 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)

[256] 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.

3) Maßnahmen	Bestehende Maßnahmen
	• Aufnahme entsprechender Hinweise in Schulungsunterlagen hinsichtlich der Nutzung des digitalen Führerscheins • Nach allen dem BMDW bzw dem BMF zum Zeitpunkt der Erstellung dieses Berichts vorliegenden Informationen ist eine Überprüfung des digitalen Führerscheins für Exekutivorgane ausschließlich im Rahmen der Verkehrskontrolle vorgesehen, zulässig und möglich.

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 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 Ausweis verwendet haben.
	Risikoquelle
	Interne technische Quellen: • Softwarearchitektur, welche etwa standardmäßig bestimmte Daten protokolliert • Softwarekonfiguration
	Risikoursache
	• Das System ist so gestaltet bzw konfiguriert, dass mehr personenbezogene Daten protokolliert werden, als zur Erfüllung legitimer Anforderungen unbedingt erforderlich ist. • Softwarebetriebsbedingte Protokollierungsanforderungen können dem Grundsatz der Datenminimierung entgegenstehen.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen), berufliche Nachteile • Finanzieller Verlust, etwa da die temporäre Abnahme eines Führerscheins bekannt wird **Immaterielle Schäden** • Rufschädigung • Verletzung der Privatsphäre • wirtschaftliche oder gesellschaftliche Nachteile • Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Eingeschränkt (2) Kommentar: Das Vorweisen des Ausweises findet offline statt (außer bei einer Verkehrskontrolle). Zu einer serverseitigen Protokollierung, wer sich	Normal (6)

		wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.	

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Ausweises findet offline statt (außer bei einer Verkehrskontrolle). Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. • Das Protokollierungskonzept wurde so gestaltet, dass die oben genannten Risikoursachen nicht zutreffen. • Backup-Konzept • Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (zB eingeschränkte Zugriffsrechte entsprechend Need-To-Know-Prinzip; Zugriffe nur nach Vier-Augen-Prinzip) • Gewährleistung der Revisionssicherheit der Protokolle: Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden. Protokolldaten sollten nicht auf den Produktivsystemen, sondern auf eigens hierfür vorgehaltenen zugriffsbeschränkten zentralen Protokollservern gespeichert werden. Die zu protokollierenden Ereignisse sollten in Echtzeit über ein sicheres Protokoll auf die Protokollserver übertragen werden. • Protokollierung des Zugriffs auf Protokolldaten • Schulung der involvierten Personen; klare Kommunikation und Aufklärung über die Einschränkung der Protokollierung und die Konsequenzen eines dienstlich nicht erforderlichen Zugriffs auf Protokolldaten (etwa Disziplinarmaßnahmen bzw Strafen) • Weder in der eAusweise-App selbst noch serverseitig besteht die Möglichkeit, die Verwendung des Führerscheins durch die Bürger*in (Verkehrskontrolle oder Führerschein vorweisen) zu protokollieren. Das FSR muss jedoch sehr wohl jeden Zugriff protokollieren, allerdings ist damit keine Risikoerhöhung für die Bürger*in durch die Verwendung des digitalen Führerscheins gegenüber der analogen Variante verbunden.	

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

5.2.6 Missbräuchliche Verwendung von Protokolldaten

1) Risikoidentifikation	**Risikobeschreibung**
	Risiko, dass Protokolldaten offengelegt bzw zweckwidrig verarbeitet werden und deshalb insbesondere bekannt wird, an welchen Stellen Betroffene ihren digitalen Ausweis verwendet haben.
	Risikoquelle
	Interne/externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) • staatliche Institutionen (Nachrichtendienste, Strafverfolgung) **Interne / externe technische Quellen:** • Softwarefehler (zB mangelhafte Verschlüsselung, offene Schnittstellen)
	Risikoursache
	• Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Unbefugte Offenlegung von und Zugang zu Daten • Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten • Verwendung der Daten durch die Verantwortlichen zu inkompatiblen Zwecken • Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler) • Verarbeitung über die Speicherfrist hinaus • Verarbeitung entgegen dem Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • Verletzung der Privatsphäre • gesellschaftliche Nachteile

	• Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3) Kommentar: Missbräuchlicher Zugriff durch Befugte möglich; ebenso unbefugter Zugriff von außen durch einen Angriff	Wesentlich (3) Kommentar: Das Vorweisen des Ausweises findet offline statt (außer bei einer Verkehrskontrolle). Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen.	Normal (9)

3) Maßnahmen	**Bestehende Maßnahmen**	
	• Privacy by Design: Das Vorweisen des Ausweises findet offline statt (außer bei einer Verkehrskontrolle). Zu einer serverseitigen Protokollierung, wer sich wem gegenüber ausweist, kann es daher architekturbedingt gar nicht kommen, weil diese Daten zu keinem Zeitpunkt auf einen Server gelangen. • Protokollierungskonzept: Die Protokollierung ist auf das technisch notwendige Minimum beschränkt; entsprechend reduziert ist auch das mit Protokolldaten verbundene potenzielle Schadensausmaß. • Bereitstellung einer sicheren Umgebung für Protokolldaten, auf welche (ausschließlich) berechtigte Nutzer*innen zugreifen können • Backup-Konzept • Rechte- und Rollenkonzept für die Verarbeitung von Protokolldaten (zB eingeschränkte Zugriffsrechte entsprechend Need-To-Know-Prinzip; Zugriffe nur nach Vier-Augen-Prinzip) • Gewährleistung der Revisionssicherheit der Protokolle: Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden. Protokolldaten sollten nicht auf den Produktivsystemen, sondern auf eigens hierfür vorgehaltenen zugriffsbeschränkten zentralen Protokollservern gespeichert werden. Die zu protokollierenden Ereignisse sollten in Echtzeit über ein sicheres Protokoll auf die Protokollserver übertragen werden.	

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

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

5.2.7 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 bei einer Verkehrskontrolle - 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 im Zuge einer Verkehrskontrolle von Exekutivorganen zur Überprüfung des digitalen Führerscheins 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 Führerscheindaten 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

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	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 das FSR • 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 das FSR 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 Unbefugter Zugriff auf das Führerscheinregister über das AWP-Backend

<table>
<tr><td rowspan="6">1) Risikoidentifikation</td><td>Risikobeschreibung</td></tr>
<tr><td>Eine unbefugte Person verschafft sich über das AWP-Backend Zugriff auf das FSR. Über das AWP-Backend ist grundsätzlich ein Zugriff auf das FSR möglich, um Führerscheindaten der jeweiligen Nutzer*innen herunterladen zu können. Zumal es sich dabei um hochqualitative Daten handelt, könnte ein Interesse daran bestehen, unbefugter Weise darauf zuzugreifen und Führerscheindaten anderer Personen zu akquirieren. Einem Angreifer, der sich Zugang zum AWP-Backend verschafft, könnte es gelingen, auf einzelne, mehrere oder alle Einträge des FSR zuzugreifen.</td></tr>
<tr><td>Risikoquelle</td></tr>
<tr><td>Interne /Externe menschliche Quellen:
Interne Mitarbeiter*innen
Externe Mitarbeiter*innen
Sonstige Dritte
Cyberkriminelle (Hacker/Schadsoftware)
Interne / externe technische Quellen:
Softwarefehler</td></tr>
<tr><td>Risikoursache</td></tr>
<tr><td>Unbefugte bzw unrechtmäßige Verarbeitung der im Führerscheinregister enthaltenen Daten</td></tr>
<tr><td>Möglicher Schaden für die betroffenen Personen</td></tr>
<tr><td>Materielle Schäden
Diskriminierung (zB bei Vertragsabschlüssen)
finanzieller Verlust (insb durch Diskriminierung aufgrund Führerscheinverlust)
Immaterielle Schäden
Rufschädigung
wirtschaftliche oder gesellschaftliche Nachteile
Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte</td></tr>
</table>

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Eintrittswahrscheinlichkeit	Schadensausmaß	Risikobewertung
	Wesentlich (3)	Maximal (4) Kommentar: Öffentlichwerden einer vorläufigen Abnahme als nicht wie-	Hoch (12)

		dergutzumachender Reputationsschaden denkbar	

3) Maßnahmen	**Bestehende Maßnahmen**
	• Über das AWP-Backend besteht kein Schreibzugriff auf das FSR, sodass eine Verfälschung der Daten auf diesem Weg ausgeschlossen ist. • Die Schnittstelle des FSR für den Führerscheinbezug durch die AWP benötigt zwingend das vbPK des VT-Bereichs der jeweiligen Bürger*in. Es ist weder eine Abfrage mittels Vorname, Nachname, Geburtsdatum noch eine Bulk-Abfrage möglich.

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

5.2.9 Nichtverfügbarkeit des Systems

1) Risikoidentifikation	**Risikobeschreibung**
	Das System steht der Nutzer*in nicht zur Verfügung und sie kann daher ihren digitalen Ausweis nicht vorweisen. Das System ist auf das reibungslose Zusammenspiel durch von verschiedenen Akteuren verwaltete Systemkomponenten angewiesen, weshalb die Verfügbarkeit eher eingeschränkt sein kann als beim physischen Ausweis. Soweit kein (physisches) Substitut mitgeführt wird, können sich verwaltungsrechtliche Folgen oder Nachteile im Rechtsverkehr ergeben.
	Risikoquelle
	Interne / Externe menschliche Quellen: • Interne Mitarbeiter*innen • Externe Mitarbeiter*innen • Betroffene • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) **Interne / externe technische Quellen:** • Softwarefehler • Endgerät • Hardwaredefekt (physikalisch) **Sonstige Quellen:** • Umwelteinflüsse (Naturgewalt)
	Risikoursache
	Der Eintritt des 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 der an sich Berechtigte es nicht schafft, sich zu authentifizieren („false negative“). Auslöser dafür kann sein, dass der biometrische Faktor nicht einsatzbereit ist oder nicht korrekt erkannt wird. Das kann z.B. verursacht werden durch: • Fehlfunktion in der Biometrie-Komponente des Smartphones (dies liegt außerhalb der Systemgrenzen, hier besteht eine Abhängigkeit von den Geräte- und Betriebssystemherstellern) • Die Biometriekomponente steht bei einer ganzen Gerätegeneration nicht mehr zur Verfügung, weil sie aufgrund einer dokumentierten Kompromittierung deaktiviert werden musste (dies liegt außerhalb der 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, 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.
	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. • Das Risiko für den Fall einer fehlenden Internetverbindung sowie für den Fall, dass das Endgerät der Nutzer*in nicht funktionsfähig ist (schadhaftes Gerät, leerer Akku etc…), wird nach § 15a Abs 1 FSG generell auf die Nutzer*in des Systems (Betroffene) übertragen. Sie wird in solchen Fällen so behandelt werden, wie wenn der Führerschein nicht mitgeführt wird,[257] was eine Geldstrafe zur Folge haben kann. **Immaterielle Schäden:** • wirtschaftliche oder gesellschaftliche Nachteile • Verweigerung des Zugangs oder Einlasses, weil sich die betroffene Person nicht ausweisen kann

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Maximal (4) Kommentar: Bei entsprechender Verbreitung sind durch Endgeräte bedingte Risikoeintritte sehr wahrscheinlich.	Wesentlich (3) Kommentar: Im Falle der Verkehrskontrolle droht die Verhängung von Bußgeldern. Bei Nutzung als Ausweis kann der Zugang zu Leistungen oder der Einlass (temporär) verwehrt sein.	Hoch (12)

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.

[257] ErläutRV 469 BlgNR 27. GP 11.

	• Stringente Außenkommunikation des Umstands, dass die zusätzliche Zurverfügungstellung des digitalen Führerscheins als moderne Inklusionsvariante einen erleichterten Zugang zu einem Verwaltungsprozess darstellt und somit gleichsam als Gegenteil eines Einschränkungsinstruments konzipiert ist • Aufklärung über Risikotragungsregel des § 15a FSG • Das Vorweisen des digitalen Führerscheins im Rahmen einer Verkehrskontrolle ist auch möglich ohne Verbindung des mobilen Endgeräts der Bürger*in zu den Servern der AWP. (Aus rechtlichen Gründen ist in regelmäßigen Abständen eine Online-Aktualisierung der Daten erforderlich.) • Es existiert ein SLA zwischen dem BMDW bzw BMF und der BRZ GmbH, das die Systemverfügbarkeit festlegt.

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

5.2.10 Unbefugte Verarbeitung biometrischer Daten

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

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

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

3) Maßnahmen	**Bestehende Maßnahmen**
	• Weder die eAusweise-App noch die serverseitige Plattform haben auf die biometrischen Daten der Nutzer*innen Zugriff. Es wird somit auch keine zentrale Datenbank mit biometrischen Merkmalen aller Nutzer*innen der eAusweise-App geführt. • Verarbeitung biometrischer Daten ausschließlich auf gesichertem und abgesondertem Modul auf dem Endgerät • Exklusive Einbindung von Endgeräten, welche über entsprechende Sicherheitsmaßnahmen verfügen • In der Regel werden bei Android-Geräten Minutien der Fingerabdrücke gespeichert und nicht der volle Fingerabdruck.[258] Bei iOS-Geräten wird allgemein nur eine mathematische Darstellung der Fingerabdrücke abgespeichert. Ein tatsächlicher Fingerabdruck kann aus diesen gespeicherten Daten nicht hergeleitet werden.[259] • Außerdem in diesem Zusammenhang ist festzuhalten, dass die Verwendung des digitalen Führerscheins durch die Bürger*in auf freiwilliger Basis geschieht. Sollten Vorbehalte gegenüber dem Einsatz biometrischer Merkmale existieren, steht nach wie vor der physische Führerschein zur Verfügung.

[258] *Garg/Yadav/Kamal*, Android Notes using Finger Print Authentication, IJSR, Volume 10 Issue 5, May 2021, DOI: 10.21275/SR21405101230, 175.
[259] https://support.apple.com/de-de/HT204587 (abgerufen am 12. 7. 2022).

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

5.2.11 Vorweisen eines gefälschten digitalen Ausweises

1) Risikoidentifikation	**Risikobeschreibung**
	Es gelingt einem Angreifer, im Fall des Offline-Use-Case (siehe Abschnitt 3.2.4) manipulierte Ausweisdaten (eine falsche Identität oder ein falsches Attribut) via Bluetooth zu übermitteln, sodass die Überprüfungs-Funktion die Manipulation nicht erkennt und die Überprüfung des manipulierten Ausweises erfolgreich verläuft.
	Risikoquelle
	Externe menschliche Quelle: • Sonstige Dritte
	Risikoursache
	Die Ursache kann entweder eine Schwachstelle in der Funktion zur Erzeugung (insbesondere Signieren) und Übermittlung der Ausweisdaten via Bluetooth oder eine Schwachstelle in der Funktion zur Überprüfung der via Bluetooth empfangenen Ausweisdaten (insbesondere Signaturprüfung) sein.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Identitätsdiebstahl oder -betrug • Psychische Schäden • Rufschädigung • Verletzung der Privatsphäre • 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 eine Eigenschaft oder die	Hoch (12)

		Identität des Gegenübers	

3) Maßnahmen	**Bestehende Maßnahmen**
	• Es sind zwei Basismaßnahmen im Einsatz, die dem entgegenwirken: ○ Die Ausweisdaten sind signiert und beim Überprüfen findet eine Signaturprüfung statt. Eine erfolgreiche Fälschung der Ausweisdaten 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 Ausweisdaten muss der Besitzer nachweisen, dass er im Besitz des privaten Schlüssels ist, dessen öffentlicher Teil im Ausweis eingebunden ist. Dies bedeutet, dass die signierten Ausweisdaten alleine nicht für den Identitätsnachweis reichen, es muss auch der Beweis erbracht werden, dass man im Besitz des Schlüssels ist, der mit dem Ausweis verknüpft wird.

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

5.2.12 Vorweisen des Ausweises einer anderen Person

1) Risikoidentifikation	**Risikobeschreibung**
	Ein Angreifer verwendet den eAusweise-App-Login einer anderen Person auf deren Endgerät oder einem anderen Endgerät, entweder mit deren Einverständnis oder gegen deren Willen, um einen an sich nicht manipulierten Ausweis dieser anderen Person vorzuweisen. Dem Angreifer gelingt es, sich als diese andere Person auszugeben, weil die überprüfende Person anhand des Ausweisfotos nicht erkennt, dass die Person auf dem Foto nicht diejenige ist, die den Ausweis vorweist. Anzumerken ist: Zu einer Risikoerhöhung kommt es aufgrund des digitalen Führerscheins gegenüber dem physischen Führerschein nur durch die (theoretische) Möglichkeit der Verwendung des eAusweise-App-Logins gegen den Willen der betroffenen Person, sodass der Angreifer nichts physisch entwenden muss. Die Problematik der Überprüfung des Gegenübers auf Übereinstimmung mit dem Ausweisfoto 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 • 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 und sollte das Foto kontrollieren; 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 Ausweises verglichen mit einem physischen Ausweis deutlich erschwert; dies ist auch gegen die bewusste Weitergabe durch rechtmäßige Ausweisinhaber*innen wirksam. • Der digitale Führerschein führt somit aufgrund der implementierten Sicherheitsmaßnahmen im Vergleich zur analogen Variante tatsächlich zu einer Reduzierung des Risikos des Vorweisens eines fremden Ausweises.

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

5.2.13 Durchbrechung der Unbeobachtbarkeit

<table>
<tr><td rowspan="8">1) Risikoidentifikation</td><td>Risikobeschreibung</td></tr>
<tr><td>Das Vorweisen des digitalen Ausweises mit der eAusweise-App (außer bei einer Verkehrskontrolle) ist bewusst so konzipiert, dass dabei keine Serverzugriffe notwendig sind („Offline-Use-Case“). Äquivalent zum Vorweisen eines physischen Ausweises soll dadurch jegliches Sammeln von Daten darüber, wann sich wer wem gegenüber ausgewiesen hat, von vornherein ausgeschlossen werden (Schutzziel der Unbeobachtbarkeit). Diesbezüglich besteht das Risiko, dass die Implementierung diesem Ziel nicht gerecht wird, und letztlich doch eine Möglichkeit gefunden wird, insbesondere über Umwege und/oder mittelbar, solche Daten – allenfalls zumindest theoretisch – zu erheben. Eine solche Möglichkeit wäre zB eine falsche Implementierung der Zertifikatsperrliste (Certificate Revocation List, CRL).</td></tr>
<tr><td>Risikoquelle</td></tr>
<tr><td>Interne / Externe menschliche Risikoquellen:
Interne Mitarbeiter*innen
Externe Mitarbeiter*innen
Sonstige Dritte
Cyberkriminelle (Hacker/Schadsoftware)
staatliche Institutionen (Nachrichtendienste, Strafverfolgung)
Interne / Externe technische Quellen
Softwarearchitektur
Softwarekonfiguration
Softwarefehler</td></tr>
<tr><td>Risikoursache</td></tr>
<tr><td>Bewusster, zielgerichteter Angriff
Protokollierung</td></tr>
<tr><td>Möglicher Schaden für die betroffenen Personen</td></tr>
<tr><td>Materielle Schäden
Diskriminierung (zB bei Vertragsabschlüssen)
berufliche Nachteile
finanzieller Verlust
Immaterielle Schäden
Rufschädigung
wirtschaftliche oder gesellschaftliche Nachteile
Verletzung der Privatsphäre</td></tr>
</table>

	• Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Maximal (4)	Hoch (12)

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

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

5.2.14 Bekanntwerden eines Führerscheinentzugs

1) Risikoidentifikation	**Risikobeschreibung**
	Einem unbefugten *Dritten* wird bekannt, dass einer betroffenen Person die Lenkberechtigung entzogen wurde.
	Risikoquelle
	Externe /Interne menschliche Risikoquellen: • Sonstige Dritte • Cyberkriminelle (Hacker/Schadsoftware) • staatliche Institutionen (Nachrichtendienste, Strafverfolgung)
	Risikoursache
	Liegt keine Lenkberechtigung (mehr) vor, muss dies bei der Überprüfung des digitalen Führerscheins zum Zweck des Nachweises der Lenkberechtigung der überprüfenden Person korrekt angezeigt werden. Die Implementierung des Systems muss sicherstellen, dass das Fehlen der Lenkberechtigung nur einer überprüfenden Person bekannt wird, der die betroffene Person die Lenkberechtigung gerade digital nachzuweisen versucht. Als Risikoursache kommt daher in erster Linie ein Fehler in dieser Implementierung infrage, welcher auch bei sorgsamster Prüfung nie ganz ausgeschlossen werden kann.
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden: • Finanzieller Verlust • Wirtschaftliche Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile **Immaterielle Schäden:** • Gesellschaftliche und soziale Nachteile (zB Rufschädigung) • Schädigung der Privatsphäre • Psychologische Schäden

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	Wesentlich (3)	Hoch (4) Kommentar: Das Bekanntwerden kann unumkehrbare Konsequenzen haben.	Hoch (12)

3) Maßnahmen	Bestehende Maßnahmen
	• Der Abruf der Information aus dem FSR, ob eine gültige Lenkberechtigung vorliegt, erfolgt nicht durch die überprüfende Person, sondern durch die betroffene Person, und diese Information kann dann innerhalb einer Gültigkeitsdauer von 30 Minuten vorgewiesen werden. Dadurch, dass Überprüfende keinen Zugriff auf die Führerscheindaten im FSR haben, wird eine wesentliche Risikoquelle von vornherein ausgeschlossen. • Die Überprüfung des Vorhandenseins einer gültigen Lenkberechtigung mittels der GWK Check-App steht andererseits nur tatsächlich befugten Personen offen, die auf einer Whitelist verzeichnet sind, die diesen den Zugang zum FSR ermöglicht.

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

5.2.15 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 BMF für den Betrieb von eGovernment-Infrastruktur.

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

5.2.16 Auslesen des Ausweises ohne Rechtsgrundlage

1) Risikoidentifikation	**Risikobeschreibung**
	Der Überprüfende hat keine Rechtsgrundlage, die Ausweisdaten der betroffenen Person zu verarbeiten (was das Überprüfen des Ausweises miteinschließt) und er dürfte daher von der betroffenen Person das Vorweisen eines Ausweises nicht verlangen. Zwar wird es stets zulässig sein, dass die betroffene Person ihren Ausweis 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). Eine Risikoerhöhung durch den digitalen Ausweis gegenüber einem physischen Ausweis ist nicht gegeben.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte • Cyberkriminelle
	Risikoursache
	• Bewusster, zielgerichteter Angriff • Druck auf die betroffene Person • Leichtgläubigkeit der betroffenen Person • Unbedarftheit, Ignoranz oder Unwissen der betroffenen Person im Umgang mit dem digitalen Ausweis • Unbefugte bzw unrechtmäßige Verarbeitung • Verarbeitung wider Treu und Glauben • Unbefugte Offenlegung von und Zugang zu Daten • Verarbeitung entgegen den Zweckbindungsgrundsatz
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust **Immaterielle Schäden** • Rufschädigung • gesellschaftliche Nachteile • Verletzung der Privatsphäre

	• Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	**Eintrittswahrscheinlichkeit**	**Schadensausmaß**	**Risikobewertung**
	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.)

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

5.2.17 Auslesen des Ausweises durch eine unautorisierte App und unbefugtes Weiterverarbeiten der Ausweisdaten

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

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

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

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

5.2.18 Weiterverarbeiten der Ausweisdaten durch die überprüfende Person

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

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

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

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

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

5.2.19 Bekanntwerden nicht erforderlicher Daten bei bloßem Altersnachweis oder Identitätsnachweis

1) Risikoidentifikation	**Risikobeschreibung**
	Der Überprüfende erhält beim Vorweisen des digitalen Führerscheins Daten, die dieser unweigerlich enthält, die aber für den Zweck des jeweiligen Vorweisens nicht unbedingt erforderlich sind, wie etwa die Klasse und das Datum der Lenkberechtigung im Zuge des Identitätsnachweises oder insbesondere die Identität der betroffenen Person im Zuge des bloßen Altersnachweises. Mit anderen Worten, die in ISO/IEC 18013 vorgesehene Möglichkeit, dass die betroffene Person nur ausgewählte Daten des digitalen Führerscheins, wie zB das Geburtsdatum, vorweisen kann (selective disclosure), ist entsprechend der geltenden Rechtslage aktuell nicht umgesetzt.
	Risikoquelle
	Externe menschliche Quellen: • Sonstige Dritte, denen die Identität oder das Alter nachgewiesen werden soll
	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

	Eintrittswahrscheinlichkeit	**Schadensausmaß**	**Risikobewertung**

2) Risikoanalyse und Bewertung (vor bzw ohne Maßnahmen)	Wesentlich (3)	Eingeschränkt (2) Kommentar: Es liegt im Ermessen der betroffenen Person, ob diese einen Ausweis zur Verfügung stellt; bei der Nutzung des digitalen Führerscheins als Ausweis wären außerdem wohl lediglich das Ausstellungsdatum, das Datum bzw die Klassen der (nicht) bestehenden Lenkberechtigung sowie der Geburtsort irrelevant. Keine Risikoerhöhung gegenüber physischem Ausweis.	Normal (6)

3) Maßnahmen	**Bestehende Maßnahmen**
	• Die Daten, die Nutzer*innen des digitalen Führerscheins einem *Dritten*, der ebenfalls die entsprechende Applikation nutzt, aus der Gesamtheit der im FSR gespeicherten Daten zur Verfügung stellen können, sind durch den Gesetzgeber durch § 15a Abs 3 FSG zumindest auf jene beschränkt, die für den Nachweis der Lenkberechtigung erforderlich sind.

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

5.2.20 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.[260] • 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
	Wesentlich (3)	Wesentlich (3)	Normal (9)

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

5.2.21 Unbewusste oder irrtümliche Datenherausgabe

1) Risikoidentifikation	**Risikobeschreibung**
	Eine betroffene Person gibt personenbezogene Daten über die eAusweise-App an einen *Dritten* weiter, ohne dass ihr das (zur Gänze) bewusst ist. Das kann irrtümlich erfolgen oder von den Daten empfangenden Dritten sogar bewusst herbeigeführt werden, denn diese haben einen Anreiz, an die hochqualitativen hoheitlichen Daten heranzukommen.
	Risikoquelle
	Interne / Externe menschliche und strukturelle Risikoquelle: • Betroffene • Sonstige Dritte
	Risikoursache
	• Unaufmerksamkeit der betroffenen Person • Unwissen der betroffenen Person • Körperliche Einschränkungen der betroffenen Person (zB Sehschwäche, motorische Einschränkungen in Bezug auf die Touch-Bedienung) • Leseschwäche der betroffenen Person • Ignoranz/Ungeduld der betroffenen Person • Intransparente Verarbeitung • Bewusste Herbeiführung des Irrtums/der unbewussten Handlung • Unübersichtliches grafisches Userinterface (GUI) bzw mangelhafte Usability der eAusweise-App • Unbeabsichtigtes Handeln: Besonders Menschen, die im Umgang mit digitalen Diensten nicht besonders geübt oder körperlich eingeschränkt sind, können rasch Vorgänge auslösen, die ihnen nicht bewusst sind und die sie eigentlich nicht wollen. Zudem ist empirisch erwiesen, dass datenschutzrechtliche Informationstexte idR kaum gelesen werden, sondern die Betroffenen einfach auf „weiter“ klicken, um möglichst rasch ans Ziel zu gelangen.[261]
	Möglicher Schaden für die betroffenen Personen
	Materielle Schäden • Diskriminierung (zB bei Vertragsabschlüssen) • berufliche Nachteile • finanzieller Verlust

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

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

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

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

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

5.2.22 Nutzung der Ökosysteme von Google und Apple

1) Risikoidentifikation	**Risikobeschreibung**
	Einzig für die Zugänglichmachung sowie die weitere Verwendung der eAusweise-App wird die technische Infrastruktur US-amerikanischer IT-Konzerne genutzt; dies bedeutet jedoch nicht, dass die Ausweisdaten selbst an diese Konzerne kommuniziert werden. Mangels alternativer Möglichkeiten begibt sich die österreichische Verwaltung damit in ein Abhängigkeitsverhältnis, allerdings ebenfalls nur in jenem Ausmaß, wie das bereits bei der ID Austria erfolgte. Diese Abhängigkeit kann sich einerseits auf die Verfügbarkeit des Systems auswirken und dazu führen, dass diese aufgrund rechtspolitischer Entwicklungen nicht mehr wie geplant gegeben ist. Darüber hinaus werden die Betroffenen damit einmal mehr dazu angehalten, sich entsprechende Konten/Accounts bei US-Unternehmen anzulegen bzw mit diesen zu kontrahieren. Über die Nutzung der Technologie bzw der Betriebs- und Ökosysteme (App-Stores) von Google und Apple kann es weiters zu einer zweck- bzw rechtswidrigen Datenverarbeitung kommen. Es besteht dann bspw das Risiko, dass die dabei (aus vertragsrechtlichen oder technischen Gründen) anfallenden Daten zu Werbezwecken weiterverarbeitet werden, da eine derartige Verwendung personenbezogener Daten als ein zentraler Bestandteil der Geschäftsmodelle dieser Unternehmen gilt. Zudem besteht das Risiko des Zugriffs auf diese Daten durch US-Sicherheitsbehörden. 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 börsennotierten US-amerikanischen IT-Konzernen, da keine eigene Distributionsplattform ohne Weiterverarbeitung der Nutzer*innendaten zu Werbezwecken verwendet wird • Datenverarbeitung wird nicht auf das notwendige Maß beschränkt; insuffiziente Umsetzung des Grundsatzes der Datenminimierung

	• Verarbeitung von personenbezogenen Daten zu inkompatiblen Zwecken (wie zB Marketing via Metadaten) • Geringeres rechtliches Schutzniveau im Sitzstaat von Google (USA). Nach FISA 702 können US-amerikanische "Anbieter elektronischer Kommunikationsdienste" (wie in 50 U.S.C. §1881(4) definiert), dazu gezwungen werden, den US-Sicherheitsbehörden Zugang zu den personenbezogenen Daten von "Nicht-US-Personen" zu gewähren.
	Möglicher Schaden für die betroffenen Personen
	Immaterielle Schäden: • Gesellschaftliche und soziale Nachteile (durch weitere Monopolisierung privater IT-Konzerne); strukturelle Schädigung der Privatsphäre (Tracking über Webseiten, Applikationen und Endgeräte hinweg); „chilling effects“, wenn Menschen davon absehen, ihre Rechte wahrzunehmen oder ihre Persönlichkeit zu entfalten

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

3) Maßnahmen	**Bestehende Maßnahmen**
	• Physische Ausweise 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.	Wesentlich (3)	Normal (9)

5.3 Diskussion der verbleibenden Risiken und Folgenabschätzung

Die vorliegende Analyse zeigt, dass – nach Ermittlung und Zuordnung der bestehenden technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen – nach derzeitigem Stand keine als hoch zu bewertenden Risiken bestehen.

Aufgrund des Tempos der technologischen Veränderung sind jedenfalls regelmäßig Überprüfungen durchzuführen, um zu bewerten, ob bzw inwiefern sich die mit der Datenverarbeitung verbundenen Risiken geändert haben und eine Anpassung der technischen und organisatorischen Maßnahmen erforderlich ist.[262]

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.[263]

Unabhängig davon soll die Datenschutzbehörde durch proaktive Vorlage dieses initialen DSFA-Berichts sowie künftig auch im Falle von Aktualisierungen stets fachlich qualifiziert auf dem Laufenden gehalten werden. Dabei gilt es – neben den hier geprüften und analysierten Risiken – gesamtgesellschaftliche Entwicklungen ebenfalls zu berücksichtigen.

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

[262] Siehe Art 5 Abs 2 sowie Art 35 Abs 11 DSGVO.
[263] 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, wobei anzumerken ist, dass entsprechend den bestehenden rechtlichen Grundlagen die in ISO/IEC 18013-5 vorgesehene Möglichkeit, dass die betroffene Person nur ausgewählte Daten des digitalen Führerscheins, wie zB das Geburtsdatum, vorweisen kann (selective disclosure), aktuell nicht umgesetzt ist;
- personenbezogene Daten einem stringenten Löschkonzept unterliegen;
- gespeicherte personenbezogene Daten strengen Zugriffsrechten unterliegen;
- der Grundsatz der Datenminimierung und das Prinzip „Privacy by Design“ insbesondere durch die Implementierung des Vorweisens des digitalen Ausweises als Vorgang, der vollständig offline, ohne die Beteiligung eines Servers stattfindet, bereits in der grundlegenden Gestaltung des Systems berücksichtigt wurden;
- die Protokollierung auf das technisch notwendige Minimum beschränkt ist und insbesondere Vorgänge des Vorweisens und Überprüfens von Ausweisen im System der Ausweisplattform nicht protokolliert werden.

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

6.2 Pflicht zur künftigen Überprüfung

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

Eine derartige Neubewertung kann sich insb durch Änderungen am gegenständlichen System, durch technische Entwicklungen, aber auch durch normative Änderungen der einschlägigen Rechtsvorschriften oder durch Gerichtsentscheidungen ergeben und im Ergebnis dazu führen, dass andere oder zusätzliche Abhilfemaßnahmen für eine datenschutzkonforme Verarbeitung vorzunehmen sind.[264]

6.3 Europäische und internationale Perspektive

Zum Zeitpunkt des Inkrafttretens des digitalen Dokumentennachweises im Führerscheinregister eignet sich der digitale Führerschein jedenfalls hinsichtlich seines Hauptzwecks zum Nachweis der entsprechenden Lenkberechtigung bei einer Verkehrskontrolle vorerst lediglich für eine Verwendung im Inland, da der österreichische Gesetzgeber nur für Fahrten im Inland festlegen konnte, dass die Verwendung des digitalen Führerscheins von der Mitführpflicht eines physischen Führerscheindokuments befreit.

Jedoch wird in weiterer Folge eine europaweite Verwendungsmöglichkeit angestrebt, weshalb die zuständige Fachabteilung des BMF an Arbeitsgruppen und Beratungen zu den Themenkreisen „EU-Wallet/ mobile driving licence (mDL)“ beteiligt ist und dort auch aktiv danach trachtet, die österreichischen Lösungen und die diese begründenden Sichtweisen den europäischen Partnern zu vermitteln und diese dafür zu gewinnen, um auf diese Art eine künftige gemeinsame europäische Lösung federführend mitzugestalten.

Darüber hinaus ist das um den österreichischen digitalen Führerschein geschaffene System dafür ausgelegt, ohne unverhältnismäßig hohen Aufwand einer in Zukunft eintretenden Änderung der Gesetzeslage in Richtung vollständige Kompatibilität zum internationalen Standard ISO/IEC 18013-5 Rechnung zu tragen und auf diese umgestellt zu werden. In diesem Fall eröffnen sich umfangreiche zusätzliche Anwendungsmöglichkeiten auch im internationalen Umfeld.

[264] 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)[265]
Abs:	Absatz
AES 256-Bit-Verschlüsselung:	Advanced Encryption Standard (Chiffre) mit Schlüssellänge von 256 Bit
Anm:	Anmerkung
Art:	Artikel
A-SIT:	Zentrum für sichere Informationstechnologie - Austria
AWP:	Ausweisplattform
BfDI:	Bundesbeauftragter für den Datenschutz und die Informationssicherheit (Deutschland); Bundesbehörde
BGBl:	Österreichisches Bundesgesetzblatt; “I” steht in diesem Zusammenhang für den ersten Teil, in dem Gesetze kundgemacht werden, in Teil “II” wiederum Verordnungen und in Teil “III” Staatsverträge.
Bitkom:	Deutscher Bundesverband der Informationswirtschaft und Telekommunikationsbranche
BlgNR:	Beilagen zu den stenographischen Protokollen des Nationalrates[266]
BMDW:	Bundesminister für Digitalisierung und Wirtschaftsstandort
BMF	Bundesministerium für Finanzen
BMG:	Bundesministeriengesetz 1986 BGBl I 1986/76

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

BMI:	Bundesminister für Inneres
BMK:	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
bPK:	bereichsspezifische Personenkennzeichen; dieses dient grundsätzlich der eindeutigen Identifikation von natürlichen Personen in einem konkreten Verwaltungsverfahren[267] und wird prinzipiell durch eine Ableitung aus der Stammzahl der betroffenen natürlichen Person gebildet, wobei die Identifizierungsfunktion auf jenen staatlichen Bereich begrenzt ist, dem die Datenverarbeitung zuzurechnen ist, in der das bPK verarbeitet werden soll (§ 9 Abs 1 E-GovG); dadurch soll sichergestellt werden, dass die Daten eines Verwaltungsbereichs über eine Person nicht mit einem anderen verknüpft werden können; die mathematischen Verfahren, die dabei eingesetzt werden (Hash-Verfahren über die Stammzahl und die Bereichskennung), werden von der Stammzahlenregisterbehörde festgelegt und im Internet veröffentlicht (§ 9 Abs 3 E-GovG); im privaten Bereich können uU ebenso bPKs gebildet werden, indem anstelle der Bereichskennung die Stammzahl oder das bPK des *Verantwortlichen* des privaten Bereichs verwendet wird (§ 14 Abs 1 E-GovG).
BRZ:	Bundesrechenzentrum GmbH
BSI:	Bundesamt für Sicherheit in der Informationstechnik; deutsche Bundesbehörde
bsph:	beispielhaft
bspw:	beispielsweise
B-VG:	Bundes-Verfassungsgesetz BGBl I 1930/1
bzgl:	bezüglich
bzw:	beziehungsweise

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

Client-Komponente:	Entweder Digitales-Amt-App, Third-Party-App oder Mobiler Web-Browser, die/der Signaturerstellungs-Requests erstellt, übermittelt und empfängt
CNIL:	französische Datenschutzbehörde
CRL:	Certificate Revocation List; Widerrufsliste (von Zertifikaten)
DSFA:	Datenschutz-Folgenabschätzung gem Art 35 DSGVO
DSFA-AV:	Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung, BGBl II 2018/108
DSFA-V:	Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, BGBl II 2018/278
DSG:	Datenschutzgesetz; Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, BGBl I 1999/165
DSGVO:	Datenschutz-Grundverordnung; VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, 1
EG-DSRL:	RL (EG) 95/46 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31
E-GovG:	E-Government-Gesetz; Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, BGBl I 2004/10
eIDAS-VO:	VO (EU) 910/2014 des Europäischen Parlaments und des Rats über elektronische Identifizierung

	und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Rechtlinie 1999/93/EG, ABl L 2014/257, 73
eIDAS 2-VO (Vorschlag):	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM(2021) 281 final 2021/0136(COD)
E-ID:	elektronischer Identitätsnachweis (s insb § 2 Z 10 E-GOVG)
E-ID-Inhaber:	E-ID-Nutzer*in nach erfolgreichem Registrierungsprozess
ErläutRV:	Erläuterungen zur Regierungsvorlage
ErwGr:	Erwägungsgrund
EuGH:	Europäischer Gerichtshof
f/ff:	folgende(r/s)/folgende
FAQ:	Frequently Asked Questions
FSG:	Führerscheingesetz BGBl I 1997/120
FSR:	Führerscheinregister
gem:	Gemäß
ggf:	gegebenenfalls
grds:	grundsätzlich
HSM:	Hardware Security Module
iaR:	in aller Regel
idF:	in der Fassung
IDP:	Identity Provider
idR:	in der Regel
IMEI:	International Mobile Equipment Identity; eindeutige Nummer des Endgeräts

IMSI:	International Mobile Subscriber Identity; eindeutige Nummer des Netzteilnehmers
insb:	insbesondere
iSd:	im Sinne der/des
iSe:	im Sinne einer/eines
ISMS:	Information Security Management System
ISO/IEC 18004:	ISO-Standard: Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification
ISO/IEC 18013:	ISO-Standard: Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application
iSv:	im Sinne von
iVm:	in Verbindung mit
iZm:	im Zusammenhang mit
leg cit:	legis citatae, der zitierten Norm
lit:	litera/literae
LPD	Landespolizeidirektion(en)
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.[268]
PVP:	Portalverbundprotokoll; wird ua dazu verwendet, um auf das SPRS zuzugreifen
Rn:	Randnummer
Rsp:	Rechtsprechung
Rz:	Randziffer
S:	Satz
SAML 2.0:	Security Assertion Markup Language 2.0
Secure Element:	dedizierte, separate, manipulationssichere Hardware zum Speichern kryptografischer Daten am Endgerät (Android Keystore bzw Secure Enclave (Apple))
SLA:	Service Level Agreement
SO:	Service Owner; Der Begriff bezeichnet die für den Service Provider verantwortliche Organisation. Das kann eine Organisation des öffentlichen Sektors (zB ein Ministerium) oder auch ein privatwirtschaftliches Unternehmen sein. Ein Service Owner kann für eine beliebige Anzahl an Service Providern verantwortlich sein.
sog:	sogenannte(n/r/s)

[268] https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund.

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[269]
StVO:	Straßenverkehrsordnung 1960 BGBl I 1960/159
SZRB:	Stammzahlenregisterbehörde; nunmehr im Wirkungsbereich des BMF[270]
tlw:	teilweise
TOM(s):	(geeignete) technische und organisatorische Maßnahmen gem DSGVO[271]
ua:	unter anderem
UDID:	Unique Device Identifier; eindeutige Gerätenummer für Apple-Produkte
uE:	unseres Erachtens
usw:	und so weiter
uU:	unter Umständen
vbPK-VT:	verschlüsseltes bereichsspezifisches Personenkennzeichen des Bereichs Verkehr und Technik
VDA:	*Vertrauensdiensteanbieter*; ein Dienst, der elektronische Signaturen, Siegel oder Zertifikate erstellt, überprüft und validiert sowie aufbewahrt[272]
vgl:	vergleiche
VO:	Verordnung

[269] Vgl § 2 Z 8 E-GOVG.
[270] Siehe erläuternd https://www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (abgerufen am 23. 8. 2022).
[271] Siehe etwa Art 24, 32 DSGVO.
[272] https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/anbieter/liste_der_vertrauensdiensteanbieter/Anbieter.de.html.

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