

BMJ - StS DS (Stabsstelle für Datenschutz)

An
alle Bundesministerien
alle Sektionen des Bundesministeriums für
Justiz
alle Datenschutzbeauftragten der
Bundesministerien
alle Ämter der Landesregierungen
die Verbindungsstelle der Bundesländer

Mag. Stefanie DÖRNHÖFER, LL.M.
Sachbearbeiterin

stefanie.doernhoefer@bmj.gv.at
+43 1 521 52-302910

Mag. Dr. Ronald BRESICH, LL.M.
Sachbearbeiter

ronald.bresich@bmj.gv.at
+43 1 521 52-302903

Per E-Mail

Museumstraße 7, 1070 Wien

E-Mail-Antworten sind bitte unter Anführung der
Geschäftszahl an team.pr@bmj.gv.at zu richten.

Geschäftszahl: 2025-0.073.307

Rundschreiben zur legislativen Ausgestaltung von Vorschriften über die Verarbeitung personenbezogener Daten

Das Bundesministerium für Justiz erlaubt sich, das beiliegende Rundschreiben für die
legislative Ausgestaltung von Vorschriften über die Verarbeitung personenbezogener
Daten zur Kenntnis zu bringen.

1. Das Rundschreiben bezieht sich auf Vorgaben, die sich aus dem Grundrecht auf Daten-
schutz (§ 1 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, sowie aus der Verord-
nung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personen-
bezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
(Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1 (im Folgenden: DSGVO),
ergeben. Allfällige weitere Vorgaben können sich aus materienspezifischen Unionsrechts-
akten ergeben.
2. Für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck
der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvoll-

streckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung – die nicht in den Anwendungsbereich der DSGVO fällt – gelten jene Teile des Rundschreibens, die auf Vorgaben des Grundrechts auf Datenschutz (§ 1 DSG) Bezug nehmen.

Soweit derartige Datenverarbeitungen den Vorgaben der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4.5.2016 S. 89 (im Folgenden: DSRL-PJ), unterliegen, sind zudem jene Teile des Rundschreibens beachtlich, die sich auf Aspekte beziehen, die in DSGVO und DSRL-PJ übereinstimmend geregelt sind (insbesondere Begriffsbestimmungen und datenschutzrechtliche Rollenverteilung).

3. Das Rundschreiben des Bundeskanzleramtes-Verfassungsdienst zur legislativen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz vom 14. Mai 2008, GZ 810.016/0001-V/3/2007, ist gegenstandslos geworden, da es auf eine Rechtslage vor dem Inkrafttreten der DSGVO abstellt.

5. Februar 2025

Für die Bundesministerin:

Mag. Dr. Eckhard RIEDL

Elektronisch gefertigt

Geschäftszahl: 2025-0.073.307

Fassung vom 5. Februar 2025

Rundschreiben

**zur legislativen Ausgestaltung von Vorschriften über
die Verarbeitung personenbezogener Daten**

Inhaltsverzeichnis

A. Legistik	4
Sachlicher und persönlicher Anwendungsbereich	4
1. Personenbezogene Daten	4
2. Geschützter Personenkreis	5
3. „Haushaltsausnahme“	5
4. Automatisierte und manuelle Datenverarbeitung.....	5
Allgemeine Vorgaben	6
5. Unionsrechtlicher Regelungsspielraum („Öffnungsklauseln“)	6
6. Gesetzesvorbehalt.....	6
7. Determinierungsgebot	7
8. Gesetzgebungskompetenz	9
9. Terminologie	9
10. Verweise.....	10
Datenschutzrechtliche Rollenverteilung	10
11. Verantwortlicher	10
12. Gemeinsam Verantwortliche	11
13. Auftragsverarbeiter	11
Spezifische Aspekte	12
14. Verarbeitungszweck.....	12
15. Verhältnismäßigkeit	13
16. Besondere Kategorien personenbezogener Daten („sensible“ Daten)	13
17. Strafrechtsrelevante Daten	14
18. Sozialversicherungsnummer und E-Government	14
19. Einwilligung im Rahmen einer gesetzlich vorgesehenen Datenverarbeitung	14
20. Übermittlung	15
21. Verarbeitung zu anderen Zwecken	16
22. Übermittlung von im Strafverfahren ermittelten Daten	16

23. Speicherbegrenzung und Löschung	17
24. Beschränkung der Rechte der betroffenen Person	17
25. Pilotprojekte und Testbetriebe	19
26. Pseudonymisierung und Archivwesen	19
27. Datenschutzbeauftragter	20
28. Vorschriften für besondere Verarbeitungssituationen.....	20
29. Strafbestimmungen.....	20
B. Materialien	21
30. Datenschutz-Folgenabschätzung	21
C. Begutachtungsverfahren	23
31. Begutachtungsfrist und Befassung des Datenschutzrates.....	23
32. Anhörung und Konsultation der Datenschutz-Aufsichtsbehörden.....	23

A. Legistik

Sachlicher und persönlicher Anwendungsbereich

1. Personenbezogene Daten

1.1. Die Vorgaben des Grundrechts auf Datenschutz (§ 1 DSG) und der DSGVO gelten nur für die Verarbeitung personenbezogener Daten; dies sind gemäß Art. 4 Z 1 DSGVO „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“)* beziehen; als identifizierbar wird eine natürliche Person angesehen, die 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“.

Im Vorfeld des Entwurfs einer Regelung über die Verarbeitung personenbezogener Daten ist daher zu prüfen, ob überhaupt personenbezogene Daten verarbeitet werden sollen.

1.2. Ein Personenbezug ist insbesondere in folgenden Fällen gegeben:

- Die betroffene Person ist (direkt oder indirekt) identifizierbar, dh. es besteht eine Rückführungsmöglichkeit auf eine konkrete Person (vgl. auch EG 26 der DSGVO).
- Es handelt sich um pseudonymisierte Daten, die unter Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können (vgl. Art. 4 Z 5 sowie EG 26 der DSGVO).
- Es handelt sich um depersonalisierte Daten, dh. es wurden zwar bestimmte Personenbezüge (zB Name) entfernt, der Personenbezug kann aber anhand anderer Daten (zB Geschäftszahl) – ggf. durch einen eingeschränkten Personenkreis – hergestellt werden.

1.3. Nicht personenbezogen sind anonymisierte Daten (einschließlich aggregierter Daten wie Statistiken), hinsichtlich derer ein Personenbezug nicht mehr hergestellt werden kann (vgl. EG 26 der DSGVO).

2. Geschützter Personenkreis

2.1. Die Vorgaben der DSGVO sowie des DSG – mit Ausnahme des in § 1 DSG geregelten Grundrechts auf Datenschutz – gelten nur für Daten, die sich auf natürliche Personen beziehen.

2.2. Das Grundrecht auf Datenschutz (§ 1 DSG) schützt neben den personenbezogenen Daten natürlicher Personen auch die Daten juristischer Personen. Dementsprechend sind die Vorgaben für Eingriffe in das Grundrecht auf Datenschutz (§ 1 Abs. 2 DSG) auch im Zusammenhang mit der Verarbeitung von Daten juristischer Personen zu beachten.

2.3. Die DSGVO und das DSG (einschließlich des Grundrechts auf Datenschutz gemäß § 1 DSG) schützen nur die personenbezogenen Daten lebender Personen. In Bezug auf die Daten von Verstorbenen sind datenschutzrechtliche Vorkehrungen nur erforderlich, soweit daraus allenfalls Rückschlüsse auf lebende Personen gezogen werden können (zB im Fall von Erbkrankheiten).

3. „Haushaltsausnahme“

3.1. Datenverarbeitungen, die natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vornehmen (zB Familienfotos im Urlaub, privates Adressverzeichnis), stellen im Regelfall einen zulässigen Eingriff in das Grundrecht auf Datenschutz (§ 1 DSG) dar und sind gemäß Art. 2 Abs. 2 lit. c DSGVO vom Anwendungsbereich der DSGVO ausgenommen (sog. „Haushaltsausnahme“).

4. Automatisierte und manuelle Datenverarbeitung

4.1. Die DSGVO und das DSG gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO und § 4 Abs. 1 DSG).

Für rein manuelle Datenverarbeitungen außerhalb eines Dateisystems sind daher Abweichungen von den Vorgaben der DSGVO und des DSG (mit Ausnahme des Grundrechts auf Datenschutz gemäß § 1 DSG) zulässig.

Allgemeine Vorgaben

5. Unionsrechtlicher Regelungsspielraum („Öffnungsklauseln“)

5.1. Die DSGVO gilt als unionsrechtliche Verordnung unmittelbar und unterliegt dem allgemeinen unionsrechtlichen Transformationsverbot. Abweichende oder wiederholende Vorschriften in nationalen Rechtsnormen (im datenschutzrechtlichen Kontext) sind daher grundsätzlich unzulässig.

Dies gilt insbesondere für die allgemeine (horizontale) Festlegung von Kriterien für die Zulässigkeit von Datenverarbeitungen.

5.2. Die DSGVO enthält jedoch gewisse Regelungsspielräume („Öffnungsklauseln“), innerhalb derer die Mitgliedstaaten zur Erlassung nationaler Vorschriften ermächtigt oder sogar verpflichtet sind.

Öffnungsklauseln bestehen insbesondere in folgenden Bereichen:

- rechtliche Verpflichtungen zur Verarbeitung personenbezogener Daten (Art. 6 Abs. 1 lit. c iVm Abs. 2 und 3 DSGVO)
- Verarbeitung personenbezogener Daten im Bereich der (schlichten) Hoheitsverwaltung (Art. 6 Abs. 1 lit. e iVm Abs. 2 und 3 DSGVO)
- Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art. 9 Abs. 1 DSGVO (Art. 9 Abs. 2 DSGVO; siehe Pkt. 16)
- spezifische Vorschriften für besondere Verarbeitungssituationen gemäß Kapitel IX der DSGVO (siehe Pkt. 28)
- Beschränkungen nach Art. 23 DSGVO (siehe Pkt. 24)

In diesen Bereichen können (im Rahmen der jeweiligen Vorgaben der DSGVO) spezifische Datenverarbeitungen materiengesetzlich geregelt werden.

6. Gesetzesvorbehalt

6.1. Nach § 1 Abs. 2 DSG sind – soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse der betroffenen Person oder mit ihrer Zustimmung erfolgt – Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK),

BGBI. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der betroffenen Personen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

6.2. Die Verarbeitung personenbezogener Daten (sowie von Daten juristischer Personen; vgl. Pkt. 2.2.) im Rahmen der Hoheitsverwaltung (durch staatliche Organe und Beliehene, einschließlich der „schlichten“ Hoheitsverwaltung) bedarf aufgrund des § 1 Abs. 2 DSG (und Art. 18 B-VG) sowie des Art. 6 Abs. 3 iVm Abs. 1 lit. e DSGVO stets einer gesetzlichen Grundlage.

Eine gesetzliche Grundlage ist auch dann erforderlich, wenn im Rahmen der (schlichten) Hoheitsverwaltung ermittelte oder sonst verarbeitete personenbezogene Daten für andere Zwecke übermittelt oder weiterverarbeitet werden sollen.

6.3. In einer Verordnung können nur bereits im Gesetz ausreichend konkret geregelte Datenverarbeitungen näher präzisiert werden. Zulässig sind beispielsweise folgende Präzisierungen:

- Präzisierung von Datenarten (zB Name, Geburtsdatum, Ausweisdaten) im Rahmen einer im Gesetz vorgesehenen Datenkategorie („Identitätsdaten“)
- Festlegung von technischen Vorgaben zur Datensicherheit (zB Verschlüsselung von Daten)
- Festlegung von Übermittlungsstichtagen

Über die gesetzliche Grundlage hinausgehende Festlegungen (zB Verarbeitung zusätzlicher Datenarten oder Übermittlung an weitere Empfänger) können in einer Verordnung nicht angeordnet werden.

7. Determinierungsgebot

7.1. Nach der Rechtsprechung des Verfassungsgerichtshofes muss eine Ermächtigungsnorm zur Verarbeitung personenbezogener Daten gemäß § 1 Abs. 2 DSG ausreichend präzise, also für jedermann vorhersehbar, regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist. Der Gesetzgeber muss nach den Vorgaben des § 1 Abs. 2 DSG somit eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle

zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden (siehe VfGH 14.12.2023, G 352/2021 mwN).

7.2. Vorschriften über die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. c und e DSGVO (rechtliche Verpflichtung des Verantwortlichen bzw. [schlichte] Hoheitsverwaltung) müssen nach Art. 6 Abs. 3 DSGVO den Zweck der Verarbeitung festlegen und sollten überdies spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO enthalten. Art. 6 Abs. 3 DSGVO nennt in diesem Zusammenhang insbesondere folgende Aspekte:

- allgemeine Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung
- verarbeitete Datenarten
- Kreis der betroffenen Personen
- an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen
- Zweckbindung
- Speicherdauer
- zulässige Verarbeitungsvorgänge und -verfahren
- Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX der DSGVO

7.3. Vor diesem Hintergrund müssen gesetzliche Regelungen über Datenverarbeitungen zumindest folgende Festlegungen enthalten:

- Wer (welcher Verantwortliche iSd Art. 4 Z 7 DSGVO) darf
- welche personenbezogenen Daten (zumindest Datenkategorien sind festzulegen, im Falle besonderer Kategorien personenbezogener Daten sind die Datenarten ausdrücklich festzulegen)
- zu welchen betroffenen Personen
- zu welchem Zweck (siehe Pkt. 14)
- in welcher Art und Weise (Verarbeitungsvorgänge und -verfahren, Verwendung eines bestimmten Datenverarbeitungssystems, Datensicherheitsmaßnahmen udgl.)
- für wie lange
- verarbeiten (ermitteln, speichern, übermitteln udgl.) und

- für welche anderen Zwecke dürfen diese übermittelt oder weiterverarbeitet werden (einschließlich Festlegung zulässiger Empfänger, ggf. Übermittlungs- bzw. Weiterverarbeitungsverbot).

8. Gesetzgebungskompetenz

8.1. Die Gesetzgebungs- und Vollziehungszuständigkeit für „allgemeine Angelegenheiten des Schutzes personenbezogener Daten“ kommt gemäß Art. 10 Abs. 1 Z 13 B-VG dem Bund zu.

8.2. Materienspezifische Regelungen über die Verarbeitung personenbezogener Daten (zB Datenverarbeitungen im Gesundheitsbereich, im Zivilverfahrensrecht oder im Archivwesen) können nicht auf den Kompetenztatbestand des Art. 10 Abs. 1 Z 13 B-VG, sondern müssen auf die Kompetenztatbestände der jeweiligen Materie gestützt werden (materien-spezifischer Datenschutz als Annexmaterie).

Zu prüfen ist daher, ob die gesetzliche Regelung einer Datenverarbeitung in kompetenz-rechtlicher Hinsicht im Bundes- oder im Landesrecht erfolgen muss.

8.3. Eine mit Landesgesetz angeordnete Übermittlung (bzw. weitere Verarbeitung) von personenbezogenen Daten aus einer bundesgesetzlich geregelten Datenverarbeitung (einschließlich Datenbanken, Register udgl.) ist nur zulässig, soweit bundesgesetzlich auch eine entsprechende Öffnungsklausel vorgesehen ist (und *vice versa*; sog. „Doppeltürmodell“).

9. Terminologie

9.1. Vorschriften über die Verarbeitung personenbezogener Daten haben die einheitliche datenschutzrechtliche Terminologie, insbesondere die Begriffsbestimmungen des Art. 4 DSGVO zu beachten.

9.2. Abweichende oder wiederholende Begriffsbestimmungen sowie Definitionen autonomer Begriffe des Unionsrechts sind unzulässig.

Insbesondere sollten die Begriffe „Anonymisierung“, „anonymisierte Daten“ und „anonyme Daten“ im Zusammenhang mit Datenverarbeitungsregelungen ausschließlich im Zusammenhang mit Informationen verwendet werden, die nicht oder nicht mehr auf eine identifizierte oder identifizierbare betroffene Person rückführbar sind (vgl. EG 26 der DSGVO). In der Rechtsordnung wird der Begriff „Anonymisierung“ (etwa im Zusammenhang mit Entscheidungsveröffentlichungen im RIS) teilweise missverständlich verwendet;

in vielen Fällen handelt es sich dabei nicht um anonyme, sondern um (ggf. depersonalisierte oder pseudonymisierte) personenbezogene Daten iSd Art. 4 Z 1 DSGVO.

10. Verweise

10.1. Die Anwendbarkeit (allenfalls auch einzelner Bestimmungen) der DSGVO darf nur in Bereichen angeordnet werden, die nicht unmittelbar der DSGVO (oder sonstigen unionsrechtlichen Vorgaben) unterliegen (siehe etwa § 4 Abs. 1 DSG).

10.2. Eine „sinngemäße“ (oder „entsprechende“) Anwendung anderer Rechtsvorschriften darf nach den Legistischen Richtlinien 1990 (LRL) nicht angeordnet werden; es ist entweder uneingeschränkt auf die anderen Rechtsvorschriften in ihrer bestehenden Fassung zu verweisen oder aber anzugeben, mit welcher Maßgabe sie angewendet werden sollen (LRL 59). Dies gilt vor dem Hintergrund des datenschutzrechtlichen Determinierungsgebots umso mehr im Zusammenhang mit Datenverarbeitungsregelungen.

Datenschutzrechtliche Rollenverteilung

11. Verantwortlicher

11.1. Zur Vermeidung von Unklarheiten und Vollzugsproblemen sollten gesetzliche Datenverarbeitungsregelungen klar erkennen lassen, wer Verantwortlicher der Verarbeitung ist.

Dabei ist insbesondere zu prüfen, ob der Verantwortliche anhand der Kriterien des Art. 4 Z 7 DSGVO („die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“) und der faktischen Umstände eindeutig bestimmbar ist.

11.2. Die Festlegung eines Verantwortlichen oder der Kriterien seiner Benennung ist nach Art. 4 Z 7 DSGVO (nur) zulässig, soweit die Zwecke und Mittel der Verarbeitung gesetzlich vorgegeben werden.

Sind mehrere Stellen in eine Datenverarbeitung involviert, ist die datenschutzrechtliche Rolle aller beteiligten Akteure zu klären. Diesfalls sollte die Rolle der einzelnen Akteure – soweit dies nach Art. 4 Z 7 DSGVO zulässig ist – im Gesetz klar festgelegt (zB „*X als Verantwortlicher (Art. 4 Z 7 DSGVO)*“, „*X und Y als gemeinsam Verantwortliche (Art. 26 DSGVO)*“) sowie näher erläutert werden.

Soll der Verantwortliche abweichend von den Kriterien des Art. 4 Z 7 DSGVO festgelegt werden, ist zu beachten, dass der Verantwortliche in der Lage sein muss, seinen datenschutzrechtlichen Verpflichtungen gemäß der DSGVO vollinhaltlich nachzukommen. Insofern ist eine von den Kriterien des Art. 4 Z 7 DSGVO abweichende Festlegung des Verantwortlichen nicht uneingeschränkt möglich.

12. Gemeinsam Verantwortliche

12.1. Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art. 26 DSGVO). Dies muss nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge haben, sodass diese auch in verschiedenen Phasen und in unterschiedlichem Ausmaß in die Verarbeitung personenbezogener Daten einbezogen sein können.

12.2. Gemeinsam Verantwortliche sind gemäß Art. 26 Abs. 1 DSGVO verpflichtet, „in einer Vereinbarung in transparenter Form fest[zulegen], wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt“. Eine solche Pflichtenverteilung kann auch im Rahmen der gesetzlichen Regelung über die Datenverarbeitung getroffen werden.

Allerdings kann die betroffene Person gemäß Art. 26 Abs. 3 DSGVO – ungeachtet der Einzelheiten der Vereinbarung gemäß Art. 26 Abs. 1 DSGVO – ihre Rechte im Rahmen der DSGVO bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen. Nachdem bislang keine entsprechende Rechtsprechung des EuGH zu dieser Bestimmung besteht, wird empfohlen, Art. 26 Abs. 3 DSGVO auch bei der Erlassung gesetzlicher Regelungen (etwa bei der Einrichtung einer gemeinsamen Anlaufstelle für die betroffene Person) zu beachten.

13. Auftragsverarbeiter

13.1. Art. 4 Z 8 DSGVO ermöglicht – anders als Art. 4 Z 7 DSGVO in Bezug auf den Verantwortlichen – keine abweichende gesetzliche Festlegung der Rolle des Auftragsverarbeiters. Dementsprechend dürfen einer als Auftragsverarbeiter ausgewiesenen Stelle keine Tätigkeiten übertragen werden, die mit dem unionsrechtlichen Verständnis des Auftragsverarbeiters nicht vereinbar sind.

Ob eine Stelle als Auftragsverarbeiter zu qualifizieren ist, ist primär anhand ihrer tatsächlichen Tätigkeit zu beurteilen (vgl. Art. 28 Abs. 10 DSGVO).

13.2. Die Zulässigkeit der Zuweisung der Rolle des Auftragsverarbeiters an ein oberstes Organ (zB einen Bundesminister) ist zweifelhaft, da der Auftragsverarbeiter hinsichtlich der Datenverarbeitung gemäß Art. 28 Abs. 3 lit. a und Art. 29 DSGVO den (datenschutzrechtlichen) Weisungen des Verantwortlichen unterliegt und dem Verantwortlichen gemäß Art. 28 Abs. 3 lit. h DSGVO ein Überprüfungs- und Inspektionsrecht zukommt. Rechtsprechung und Lehre gehen davon aus, dass die in Art. 19 Abs. 1 B-VG genannten obersten Organe „nicht der Leitung, insb der Aufsicht und den Weisungen (und sonstigen Anordnungen) anderer Organe unterworfen sind, soweit nicht verfassungsgesetzlich anderes bestimmt ist“ (siehe *Raschauer*, Art. 19 Abs. 1 B-VG in Korinek/Holoubek et al [Hrsg.], Österreichisches Bundesverfassungsrecht Rz 52). Insoweit besteht ein Spannungsverhältnis zwischen der datenschutzrechtlichen Rolle als Auftragsverarbeiter und der Stellung als oberstes Organ im Sinne des B-VG.

Dementsprechend wird empfohlen, entweder ein anderes Verwaltungsorgan als Auftragsverarbeiter zu wählen oder oberste Organe nur als (ggf. gemeinsam) Verantwortliche iSd Art. 4 Z 7 DSGVO festzulegen.

13.3. Art. 28 Abs. 3 DSGVO sieht nähere Vorgaben über die Auftragsverarbeitung vor, die insbesondere im Bereich der (schlichten) Hoheitsverwaltung im Gesetz festzulegen sind. Die Auftragsverarbeiter sollten in diesem Fall gesetzlich zumindest dazu verpflichtet werden, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen.

Spezifische Aspekte

14. Verarbeitungszweck

14.1. Gesetzliche Datenverarbeitungsregelungen müssen den jeweiligen Zweck der Datenverarbeitung im Gesetz festlegen.

Dabei ist insbesondere der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) zu beachten, demzufolge personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

14.2. Im Bereich der (schlichten) Hoheitsverwaltung darf die Verarbeitung personenbezogener Daten gemäß § 1 Abs. 2 DSG nur aus den in Art. 8 Abs. 2 EMRK genannten Gründen (nationale Sicherheit, öffentliche Ruhe und Ordnung, wirtschaftliches Wohl des Landes, Verteidigung der Ordnung und Verhinderung von strafbaren Handlungen, Schutz der

Gesundheit und der Moral oder Schutz der Rechte und Freiheiten anderer) vorgesehen werden. Der Verarbeitungszweck muss somit einem dieser Gründe entsprechen.

15. Verhältnismäßigkeit

15.1. Im Lichte des Verhältnismäßigkeitsgrundsatzes (§ 1 Abs. 2 DSG) sowie des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) darf die Verarbeitung personenbezogener Daten nur im zur Zweckerreichung erforderlichen Umfang vorgesehen werden.

15.2. Vorschriften über die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. c und e DSGVO (rechtliche Verpflichtung des Verantwortlichen bzw. [schlichte] Hoheitsverwaltung) müssen zudem gemäß Art. 6 Abs. 3 DSGVO ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

16. Besondere Kategorien personenbezogener Daten („sensible“ Daten)

16.1. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (besondere Kategorien personenbezogener Daten iSd Art. 9 Abs. 1 DSGVO bzw. besonders schutzwürdige Daten iSd § 1 Abs. 2 DSG) unterliegt erhöhten datenschutzrechtlichen Anforderungen.

Die genannten Daten dürfen nur in den in Art. 9 Abs. 2 DSGVO abschließend festgelegten Fällen verarbeitet werden. Vorschriften über die Verarbeitung besonderer Kategorien personenbezogener Daten haben die Vorgaben des jeweiligen Ausnahmetatbestands des Art. 9 Abs. 2 DSGVO zu berücksichtigen.

In den Erläuterungen sollte angeführt werden, auf welchen Tatbestand des Art. 9 Abs. 2 DSGVO die vorgesehene Verarbeitung der jeweiligen besonderen Kategorien personenbezogener Daten gestützt wird.

16.2. Im Bereich der (schlichten) Hoheitsverwaltung darf die Verarbeitung der genannten Daten nur zur Wahrung wichtiger öffentlicher Interessen vorgesehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der betroffenen Person festgelegt werden (§ 1 Abs. 2 zweiter Satz DSG).

Im Gesetz sollten insbesondere grundlegende Datensicherheitsmaßnahmen iSd Art. 32 DSGVO (zB Protokollierungspflicht, Zugangs- und Zugriffsbeschränkungen) vorgegeben werden. Eine allgemeine Verpflichtung zur Ergreifung angemessener Datensicherheitsmaßnahmen ist nicht ausreichend.

16.3. Zu verarbeitende besondere Kategorien personenbezogener Daten sind im Gesetz ausdrücklich und abschließend anzuführen. Dabei sollte geregelt werden, welche konkrete Datenart (zB Blutgruppe als Gesundheitsdatum) verarbeitet werden muss, um den angestrebten Zweck zu erreichen.

17. Strafrechtsrelevante Daten

17.1. Rechtsvorschriften, die die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (sog. strafrechtsrelevante Daten) – dies können auch personenbezogene Daten über Verwaltungsstrafverfahren sein – regeln, müssen gemäß Art. 10 DSGVO geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsehen.

17.2. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nach Art. 10 DSGVO nur unter behördlicher Aufsicht geführt werden.

18. Sozialversicherungsnummer und E-Government

18.1. Die Verwendung der Sozialversicherungsnummer für Bereiche, die nicht in der Ingerenz der Sozialversicherung liegen, steht in einem Spannungsverhältnis zum Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO). Hier ist den E-Government-Lösungen des Bundes (Verwendung des bereichsspezifischen Personenkennzeichens – bPK) unter Gewähr der höchstmöglichen Datensicherheitsmaßnahmen der Vorzug zu geben.

18.2. Bei der Anordnung der Verarbeitung von bPK sollte möglichst auch im Gesetz geregelt werden, ob allenfalls ein verschlüsseltes bPK zu verarbeiten (bzw. zu übermitteln) ist und aus welchem Bereich das bPK zu verwenden ist (siehe diesbezüglich auch die E-Government-Bereichsabgrenzungsverordnung – E-Gov-BerAbgrV, BGBl. II Nr. 289/2004).

19. Einwilligung im Rahmen einer gesetzlich vorgesehenen Datenverarbeitung

19.1. Der Begriff „Einwilligung“ sollte im Datenverarbeitungskontext (nur) dann verwendet werden, wenn es sich um eine datenschutzrechtliche Einwilligung iSd Art. 4 Z 11 DSGVO iVm Art. 7 DSGVO handelt.

Nach Art. 4 Z 11 DSGVO ist die Einwilligung eine „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Die Einwilligung unterliegt den Bedingungen des Art. 7 DSGVO und kann nach Art. 7 Abs. 3 DSGVO jederzeit widerrufen werden.

19.2. Für Datenverarbeitungen, die unmittelbar auf die Rechtsgrundlage der (ausdrücklichen) Einwilligung (Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO) gestützt werden können, ist die gesetzliche Festlegung einer Einwilligung grundsätzlich nicht erforderlich.

Im Bereich der (schlichten) Hoheitsverwaltung können Datenverarbeitungen nicht unmittelbar auf die Rechtsgrundlage der Einwilligung gestützt werden (siehe Pkt. 6.2.).

19.3. Im Zusammenhang mit gesetzlich geregelten Datenverarbeitungen (auch im Bereich der [schlichten] Hoheitsverwaltung) kann eine positive Willensbekundung der betroffenen Person als zusätzliche Voraussetzung der Datenverarbeitung vorgesehen werden.

Diesfalls wäre zur Vermeidung von Missverständnissen und unerwünschten Rechtsfolgen (insb. Widerrufsmöglichkeit der datenschutzrechtlichen Einwilligung nach Art. 7 Abs. 3 DSGVO) auf andere Begriffe als „Einwilligung“ (etwa „Zustimmung“ oder „Einverständnis“) zurückzugreifen und in den Erläuterungen klarzustellen, dass es sich dabei nicht um eine datenschutzrechtliche Einwilligung handelt.

19.4. Soweit eine Datenverarbeitungsregelung auf die Zustimmung, das Einverständnis o.Ä. der betroffenen Person Bezug nimmt, sollte in den Erläuterungen klargelegt werden, auf welche Rechtsgrundlage sich die Datenverarbeitung stützt (insb. Gesetz iSd Art. 6 Abs. 2 und 3 iVm Abs. 1 lit. c oder e DSGVO bzw. sonstige Öffnungsklausel der DSGVO).

20. Übermittlung

20.1. Zusätzlich zu den allgemeinen Vorgaben für gesetzliche Verarbeitungen personenbezogener Daten sollte der Empfänger der Datenübermittlung im Gesetz genannt werden.

Soweit sich die datenschutzrechtliche Rollenverteilung nicht klar aus der gesetzlichen Regelung ergibt, sollte in den Erläuterungen dargelegt werden, ob der Empfänger der Daten Verantwortlicher (Art. 4 Z 7 DSGVO) oder Auftragsverarbeiter (Art. 4 Z 8 DSGVO) ist.

20.2. Im Falle einer gesetzlichen Regelung über die Übermittlung personenbezogener Daten an Drittländer (zB ausländische Behörden) oder internationale Organisationen sind die Vorgaben des Kapitel V der DSGVO einzuhalten.

21. Verarbeitung zu anderen Zwecken

21.1. Die Weiterverarbeitung personenbezogener Daten zu anderen Zwecken unterliegt grundsätzlich denselben Vorgaben wie die erstmalige Verarbeitung. Art. 6 Abs. 4 DSGVO sieht gewisse Erleichterungen für die Weiterverarbeitung von personenbezogenen Daten zu „kompatiblen Zwecken“ vor.

Eine Weiterverarbeitung im Rahmen der (schlichten) Hoheitsverwaltung bedarf jedenfalls einer gesetzlichen Rechtsgrundlage (siehe Pkt. 6.2.).

21.2. Allfällige Weiterverarbeitungen dürfen nur im erforderlichen und verhältnismäßigen Ausmaß vorgesehen werden. In diesem Zusammenhang ist insbesondere der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) zu beachten.

Soweit horizontale Regelungen in anderen Materien- oder Verfahrensgesetzen eine überschießende Weiterverarbeitung ermöglichen würden, sind ausdrücklich Weiterverarbeitungsbeschränkungen bzw. Weiterverarbeitungsverbote zu verankern.

22. Übermittlung von im Strafverfahren ermittelten Daten

22.1. Eine Übermittlungsermächtigung bzw. -pflicht für im Strafverfahren ermittelte personenbezogene Daten zu anderen Zwecken muss im Gesetz ausdrücklich vorgesehen sein und darf nur insoweit angeordnet werden, als die damit verfolgten Interessen das Geheimhaltungsinteresse der betroffenen Person überwiegen und die Maßnahme das geringste Mittel zur Erreichung des Zwecks darstellt. Dabei ist bereits auf gesetzlicher Ebene möglichst präzise festzulegen, welche personenbezogenen Daten durch welche Strafverfolgungsbehörden übermittelt werden dürfen. Insbesondere sollte geprüft werden, ob eine Einschränkung auf bestimmte Datenarten oder einen bestimmten betroffenen Personenkreis möglich ist oder eine Übermittlung bestimmter Kategorien personenbezogener Daten oder von personenbezogenen Daten aus bestimmten Ermittlungsmaßnahmen bereits auf gesetzlicher Ebene ausgeschlossen werden kann.

Vor dem Hintergrund der besonderen Sensibilität von im Strafverfahren ermittelten Daten und der Eingriffsintensität der in der StPO vorgesehenen Ermittlungsmaßnahmen (zB kör-

perliche oder molekulargenetische Untersuchung, Überwachung von Nachrichten) erscheinen Einschränkungen der Datenkategorien geboten, um die datenschutzrechtliche Verhältnismäßigkeitsabwägung bereits auf gesetzlicher Ebene sicherzustellen.

23. Speicherbegrenzung und Löschung

23.1. Im Gesetz sollte eine konkrete (Höchst-)Aufbewahrungsdauer von personenbezogenen Daten für den Verantwortlichen festgelegt werden. Der Anknüpfungspunkt für den Beginn der Aufbewahrungsfrist muss sich aus dem Gesetz klar ergeben.

Soweit die gesetzliche Festlegung einer konkreten Aufbewahrungsdauer nicht möglich ist, sollte zumindest in den Erläuterungen dargelegt werden, nach welchen Kriterien der Verantwortliche zu entscheiden hat, dass die personenbezogenen Daten zu löschen sind (zB nach Eintritt einer konkreten Bedingung).

23.2. Allgemeine Lösungsverpflichtungen, die bereits unmittelbar aufgrund der DSGVO bestehen (etwa die nach Art. 17 Abs. 1 lit. a DSGVO bestehende Verpflichtung zur unverzüglichen Löschung, wenn die Daten für den Verarbeitungszweck nicht mehr benötigt werden), dürfen aufgrund des Transformationsverbots nicht neuerlich verankert werden.

24. Beschränkung der Rechte der betroffenen Person

24.1. Art. 23 DSGVO regelt, unter welchen Voraussetzungen die Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, die Pflichten und Rechte gemäß

- Art. 12 bis 22 DSGVO (im Zusammenhang mit den datenschutzrechtlichen Betroffenenrechten auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruchsrecht sowie Rechte iZm der automatisierten Entscheidung im Einzelfall einschließlich Profiling),
- Art. 34 DSGVO (Benachrichtigung der betroffenen Person über eine Verletzung des Schutzes personenbezogener Daten) sowie
- Art. 5 DSGVO, insofern dessen Bestimmungen den in den Art. 12 bis 22 DSGVO vorgesehenen Rechten und Pflichten entsprechen,

im Wege von Gesetzgebungsmaßnahmen beschränken dürfen.

Eine derartige Beschränkung ist nur zulässig, sofern sie den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Sicherstellung der in Art. 23 Abs. 1 DSGVO abschließend aufgezählten Ziele darstellt. Diese umfassen:

- die nationale Sicherheit (lit. a)
- die Landesverteidigung (lit. b)
- die öffentliche Sicherheit (lit. c)
- die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (lit. d)
- den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit (lit. e)
- den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren (lit. f)
- die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe (lit. g)
- Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind (lit. h)
- den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen (lit. i)
- die Durchsetzung zivilrechtlicher Ansprüche (lit. j)

24.2. Im Falle der gesetzlichen Beschränkung der Rechte der betroffenen Person sollte in den Erläuterungen dargelegt und begründet werden, aufgrund welches Ausnahmetatbestandes des Art. 23 Abs. 1 lit. a bis j DSGVO die konkrete Beschränkung erforderlich ist.

24.3. Gesetzliche Beschränkungen der Betroffenenrechte sind auf das zur Zweckerreichung unbedingt erforderliche Ausmaß einzuschränken und nach Möglichkeit zu befristen.

In den Erläuterungen sind die Erforderlichkeit und Verhältnismäßigkeit der Beschränkung(en) in Bezug auf jedes davon umfasste Betroffenenrecht im Einzelnen darzulegen und zu begründen.

24.4. Gesetzliche Regelungen zur Beschränkung von Betroffenenrechten iSd Art. 23 Abs. 1 DSGVO müssen insbesondere gegebenenfalls spezifische Vorschriften enthalten, zumindest in Bezug auf

- die Zwecke der Verarbeitung oder die Verarbeitungskategorien,
- die Kategorien personenbezogener Daten,
- den Umfang der vorgenommenen Beschränkungen,
- die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,
- die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,
- die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,
- die Risiken für die Rechte und Freiheiten der betroffenen Personen und
- das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

25. Pilotprojekte und Testbetriebe

25.1. Die DSGVO und das DSG sehen keine Ausnahmen bzw. Erleichterungen für die Verarbeitung personenbezogener Echtdaten im Rahmen eines Pilotprojekts oder Testbetriebs vor. Dementsprechend kann auch dafür ein umfassendes gesetzliches Regelungsregime erforderlich sein.

26. Pseudonymisierung und Archivwesen

26.1. Die (gesetzliche Anordnung zur) Pseudonymisierung personenbezogener Daten stellt eine Datensicherheitsmaßnahme (Art. 32 Abs. 1 lit. a DSGVO) dar, beseitigt jedoch iSd Definition in Art. 4 Z 5 DSGVO nicht den Personenbezug (siehe Pkt. 1.2.). Pseudonymisierte Daten sind somit personenbezogene Daten. Die Pseudonymisierung kann daher das Löschen von nicht mehr erforderlichen Daten nicht ersetzen.

26.2. Im Falle der gesetzlichen Anordnung einer Pseudonymisierung sollte auch geregelt (oder zumindest in den Erläuterungen dargelegt) werden, welcher Identifikator als Pseudonym verwendet bzw. wie dieser gebildet wird.

26.3. Archivrechtliche Vorschriften über die Aufbewahrung oder Übermittlung von Daten (zB an das Österreichische Staatsarchiv) können einer Löschung personenbezogener Daten entgegenstehen und ein Rechtsgrund zur weiteren Aufbewahrung sein.

27. Datenschutzbeauftragter

27.1. Dem Datenschutzbeauftragten können zusätzlich zu den in Art. 37 ff DSGVO genannten Aufgaben und Pflichten weitere Aufgaben und Pflichten übertragen werden, soweit diese nicht zu einem Interessenkonflikt führen (vgl. Art. 38 Abs. 6 DSGVO).

28. Vorschriften für besondere Verarbeitungssituationen

28.1. Kapitel IX der DSGVO sieht Öffnungsklauseln für folgende besondere Verarbeitungssituationen vor:

- Meinungsäußerungs- und Informationsfreiheit (Art. 85 DSGVO)
- Zugang der Öffentlichkeit zu amtlichen Dokumenten (Art. 86 DSGVO)
- Nationale Kennziffer (Art. 87 DSGVO)
- Beschäftigungskontext (Art. 88 DSGVO)
- Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Art. 89 DSGVO)
- Geheimhaltungspflichten (Art. 90 DSGVO)
- Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften (Art. 91 DSGVO)

Auf diese Öffnungsklauseln gestützte Datenverarbeitungsregelungen müssen die in den jeweiligen Bestimmungen vorgesehenen Voraussetzungen erfüllen (zB Schaffung von geeigneten Garantien gemäß Art. 89 DSGVO) und auch die sonstigen Verpflichtungen der DSGVO (insb. Kapitel II und III DSGVO) einhalten. In den Erläuterungen sollte das Vorliegen der betreffenden Voraussetzungen dargelegt werden.

29. Strafbestimmungen

29.1. Die materiellen Voraussetzungen für die Verhängung von Geldbußen sind in Art. 83 DSGVO abschließend geregelt. Für datenschutzrechtliche Verstöße, die unter Art. 83 DSGVO fallen, dürfen daher keine gesonderten Strafbestimmungen angeordnet werden. Andere Sanktionen für Verstöße gegen die DSGVO – insbesondere für Verstöße, die keiner Geldbuße gemäß Art. 83 DSGVO unterliegen – können festgelegt werden (Art. 84 DSGVO).

B. Materialien

30. Datenschutz-Folgenabschätzung

30.1. Im Vorblatt zur (vereinfachten) Wirkungsorientierten Folgenabschätzung ist darzulegen, ob und gegebenenfalls von wem eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO vorzunehmen ist oder aus welchem Grund diese unterbleiben kann.

30.2. Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 1 DSGVO erforderlich,

- wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, insbesondere in den Fällen des Abs. 3:
 - systematische und umfassende Bewertung auf Basis automatisierter Verarbeitung einschließlich Profiling,
 - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder
 - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- sowie für Verarbeitungsvorgänge gemäß der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018.

In der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018, genannte Datenverarbeitungen erfordern keine Datenschutz-Folgenabschätzung.

30.3. Die Durchführung der Datenschutz-Folgenabschätzung obliegt gemäß Art. 35 DSGVO dem Verantwortlichen der Datenverarbeitung.

Art. 35 Abs. 10 DSGVO ermöglicht abweichend davon unter bestimmten Voraussetzungen eine Vorwegnahme der Datenschutz-Folgenabschätzung im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass einer gesetzlichen Rechtsgrundlage für eine Datenverarbeitung.

Eine unvollständige oder erst nach Erlass der Rechtsgrundlage vorgenommene Datenschutz-Folgenabschätzung entspricht nicht den Vorgaben des Art. 35 Abs. 10 DSGVO. In

diesen Fällen trifft die Verpflichtung zur (vollständigen) Durchführung der Datenschutz-Folgenabschätzung (wieder) den jeweiligen Verantwortlichen.

30.4. Die Durchführung einer vorweggenommenen Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 10 DSGVO sollte in den Erläuterungen erfolgen. Eine Veröffentlichung auf der Website eines Ressorts genügt den Anforderungen des Art. 35 Abs. 10 DSGVO nicht.

30.5. Eine (vorweggenommene) Datenschutz-Folgenabschätzung muss gemäß Art. 35 Abs. 7 DSGVO zumindest folgende Elemente enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen (lit. a)
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (lit. b)
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DSGVO (lit. c)
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird (lit. d)

C. Begutachtungsverfahren

31. Begutachtungsfrist und Befassung des Datenschutzrates

31.1. Dem Datenschutzrat ist Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien, soweit diese datenschutzrechtlich von Bedeutung sind, sowie zu Verordnungen im Vollzugsbereich des Bundes, die wesentliche Fragen des Datenschutzes betreffen, zu geben (§ 14 Abs. 2 Z 3 DSG).

Im Falle einer zu kurz bemessenen Frist (zB nur wenige Tage) kann keine Sitzung des Datenschutzrates stattfinden, womit ihm auch die nach § 14 Abs. 2 Z 3 DSG zustehende Gelegenheit zur Stellungnahme genommen wird.

32. Anhörung und Konsultation der Datenschutz-Aufsichtsbehörden

32.1. Vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, sind die Datenschutzbehörde und das Parlamentarische Datenschutzkomitee anzuhören (§ 21 Abs. 1 zweiter Satz [iVm § 35e Abs. 2] DSG).

32.2. Eine Verpflichtung zur vorherigen Konsultation der Datenschutzbehörde bzw. des Parlamentarischen Datenschutzkomitees besteht, wenn aus einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft (Art. 36 DSGVO).