Gesamte Rechtsvorschrift für Datenschutzgesetz, Fassung vom 27.11.2026

Umsetzungshinweis für folgende Bestimmung

CELEX-Nr.: 32023L0977

Langtitel

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)
StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CELEX-Nr.: 395L0046]

Änderung

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81. BR: 6458 AB 6459 S. 681.)
BGBl. I Nr. 13/2005 (NR: GP XXII IA 515/A AB 821 S. 96. BR: AB 7228 S. 719.)
BGBl. I Nr. 2/2008 (1. BVRBG) (NR: GP XXIII RV 314 AB 370 S. 41. BR: 7799 AB 7830 S. 751.)
BGBl. I Nr. 133/2009 (NR: GP XXIV RV 472 AB 531 S. 49. BR: 8220 AB 8225 S. 780.)
BGBl. I Nr. 135/2009 (NR: GP XXIV RV 485 AB 558 S. 49. BR: 8217 AB 8228 S. 780.)
BGBl. I Nr. 112/2011 (NR: GP XXIV RV 1494 AB 1500 S. 130. BR: 8602 AB 8603 S. 802.)
[CELEX-Nr.: 32009L0133, 32010L0024]
BGBl. I Nr. 51/2012 (NR: GP XXIV RV 1618 AB 1771 S. 155. BR: 8730 AB 8731 S. 809.)
BGBl. I Nr. 57/2013 (NR: GP XXIV RV 2131 AB 2245 S. 194. BR: AB 8940 S. 819.)
BGBl. I Nr. 83/2013 (NR: GP XXIV RV 2168 AB 2268 S. 200. BR: AB 8968 S. 820.)
[CELEX-Nr.: 31995L0046]
BGBl. I Nr. 132/2015 (VfGH)
BGBl. I Nr. 120/2017 (NR: GP XXV RV 1664 AB 1761 S. 190. BR: 9824 AB 9856 S. 871.)
[CELEX-Nr.: 32016L0680]
BGBl. I Nr. 23/2018 (NR: GP XXVI IA 188/A AB 99 S. 21. BR: AB 9958 S. 879.)
BGBl. I Nr. 24/2018 (NR: GP XXVI IA 189/A AB 98 S. 21. BR: AB 9948 S. 879.)
BGBl. I Nr. 14/2019 (NR: GP XXVI RV 301 AB 463 S. 57. BR: AB 10104 S. 888.)
BGBl. I Nr. 148/2021 (NR: GP XXVII RV 937 AB 963 S. 117. BR: AB 10729 S. 929.)
BGBl. I Nr. 2/2023 (VfGH)
BGBl. I Nr. 62/2024 (NR: GP XXVII IA 4031/A AB 2566 S. 266. BR: 11496 AB 11507 S. 968.)
BGBl. I Nr. 70/2024 (NR: GP XXVII AB 2594 S. 268. BR: AB 11514 S. 968.)
BGBl. I Nr. 50/2025 (NR: GP XXVIII RV 129 AB 151 S. 35. BR: 11651 AB 11654 S. 980.)

Präambel/Promulgationsklausel

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Artikel 1
(Verfassungsbestimmung)

§ 1 Grundrecht auf Datenschutz
(Anm.: §§ 2 und 3 aufgehoben durch BGBl. I Nr. 14/2019)

Artikel 2

1. Hauptstück
Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen

1. Abschnitt
Allgemeine Bestimmungen

§ 4. Anwendungsbereich und Durchführungsbestimmung
§ 5. Datenschutzbeauftragter
§ 6. Datengeheimnis

2. Abschnitt
Datenverarbeitungen zu spezifischen Zwecken

§ 7. Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke
§ 8. Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen
§ 9. Freiheit der Meinungsäußerung und Informationsfreiheit
§ 10. Verarbeitung personenbezogener Daten im Katastrophenfall
§ 11. Verwarnung durch die Datenschutzbehörde

3. Abschnitt
Bildverarbeitung

§ 12. Zulässigkeit der Bildaufnahme
§ 13. Besondere Datensicherheitsmaßnahmen und Kennzeichnung

2. Hauptstück
Organe

1. Abschnitt
Datenschutzrat

§ 14. Einrichtung und Aufgaben
§ 15. Zusammensetzung
§ 16. Vorsitz und Geschäftsführung
§ 17. Sitzungen und Beschlussfassung

2. Abschnitt
Datenschutzbehörde

§ 18. Einrichtung
§ 19. Unabhängigkeit
§ 20. Leiter der Datenschutzbehörde
§ 21. Aufgaben
§ 22. Befugnisse
§ 23. Tätigkeitsbericht und Veröffentlichung von Entscheidungen

3. Abschnitt
Rechtsbehelfe, Haftung und Sanktionen

§ 24. Beschwerde an die Datenschutzbehörde
§ 25. Begleitende Maßnahmen im Beschwerdeverfahren
§ 26. Verantwortliche des öffentlichen und des privaten Bereichs
§ 27. Beschwerde an das Bundesverwaltungsgericht
§ 28. Vertretung von betroffenen Personen
§ 29. Haftung und Recht auf Schadenersatz
§ 30. Allgemeine Bedingungen für die Verhängung von Geldbußen

4. Abschnitt
Aufsichtsbehörde nach der Richtlinie (EU) 2016/680

§ 31. Datenschutzbehörde
§ 32. Aufgaben der Datenschutzbehörde
§ 33. Befugnisse der Datenschutzbehörde
§ 34. Allgemeine Bestimmungen

5. Abschnitt
Besondere Befugnisse der Datenschutzbehörde

§ 35.

6. Abschnitt
Parlamentarisches Datenschutzkomitee

§ 35a. Einrichtung
§ 35b. Mitglieder
§ 35c. Unabhängigkeit
§ 35d. Vorsitz und Beschlussfassung
§ 35e. Aufgaben, Befugnisse, Tätigkeitsbericht und Veröffentlichung von Entscheidungen
§ 35f. Beschwerde an das Parlamentarische Datenschutzkomitee
§ 35g. Parteistellung, Rechtsmittellegitimation und Geheimhaltungsverpflichtung
§ 35h. Beschwerde an das Bundesverwaltungsgericht

7. Abschnitt
Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle und Zusammenarbeit der Aufsichtsbehörden in Angelegenheiten der Europäischen Union

§ 35i. Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle
§ 35j. Zusammenarbeit und Kohärenz

3. Hauptstück
Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des Verfassungsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs

1. Abschnitt
Allgemeine Bestimmungen

§ 36. Anwendungsbereich und Begriffsbestimmungen
§ 37. Grundsätze für die Datenverarbeitung, Kategorisierung und Datenqualität
§ 38. Rechtmäßigkeit der Verarbeitung
§ 39. Verarbeitung besonderer Kategorien personenbezogener Daten
§ 40. Verarbeitung für andere Zwecke und Übermittlung
§ 41. Automatisierte Entscheidungsfindung im Einzelfall

2. Abschnitt
Rechte der betroffenen Person

§ 42. Grundsätze
§ 43. Information der betroffenen Person
§ 44. Auskunftsrecht der betroffenen Person
§ 45. Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung

3. Abschnitt
Verantwortlicher und Auftragsverarbeiter

§ 46. Pflichten des Verantwortlichen
§ 47. Gemeinsam Verantwortliche
§ 48. Auftragsverarbeiter und Aufsicht über die Verarbeitung
§ 49. Verzeichnis von Verarbeitungstätigkeiten
§ 50. Protokollierung
§ 51. Zusammenarbeit mit der Datenschutzbehörde
§ 52. Datenschutz-Folgenabschätzung
§ 53. Vorherige Konsultation der Datenschutzbehörde
§ 54. Datensicherheitsmaßnahmen
§ 55. Meldung von Verletzungen an die Datenschutzbehörde
§ 56. Benachrichtigung der betroffenen Person von Verletzungen
§ 57. Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

4. Abschnitt
Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

§ 58. Allgemeine Grundsätze für die Übermittlung personenbezogener Daten
§ 59. Datenübermittlung an Drittländer oder internationale Organisationen

(Anm.: § 60. mit Ablauf des 15.1.2019 außer Kraft getreten, vgl. BGBl. I Nr. 14/2019
§ 61. aufgehoben durch BGBl. I Nr. 14/2019)

4. Hauptstück
Besondere Strafbestimmungen

§ 62. Verwaltungsstrafbestimmung
§ 63. Datenverarbeitung in Gewinn- oder Schädigungsabsicht

5. Hauptstück
Schlussbestimmungen

§ 64. Durchführung und Umsetzung von Rechtsakten der EU
§ 65. Sprachliche Gleichbehandlung
§ 66. Erlassung von Verordnungen
§ 67. Verweisungen
§ 68. Vollziehung
§ 69. Übergangsbestimmungen
§ 70. Inkrafttreten

Text

Artikel 1
(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind 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), BGBl. 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 festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(Anm.: Abs. 5 aufgehoben durch BGBl. I Nr. 51/2012)

Artikel 2

1. Hauptstück
Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen

1. Abschnitt
Allgemeine Bestimmungen

Anwendungsbereich und Durchführungsbestimmung

§ 4. (1) Die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener 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) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten natürlicher Personen sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

(2) Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

(3) Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
2. sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet.

(4) Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das vierzehnte Lebensjahr vollendet hat.

(5) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem hoheitlich tätigen Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

(6) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde.

(Anm.: Abs. 7 aufgehoben durch Art. 5 Z 3, BGBl. I Nr. 14/2019)

Datenschutzbeauftragter

§ 5. (1) Der Datenschutzbeauftragte und die für ihn tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten bei der Erfüllung der Aufgaben zur Geheimhaltung verpflichtet. Dies gilt insbesondere in Bezug auf die Identität betroffener Personen, die sich an den Datenschutzbeauftragten gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, es sei denn, es erfolgte eine ausdrückliche Entbindung von der Verschwiegenheit durch die betroffene Person. Der Datenschutzbeauftragte und die für ihn tätigen Personen dürfen die zugänglich gemachten Informationen ausschließlich für die Erfüllung der Aufgaben verwenden und sind auch nach Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet.

(2) Erhält ein Datenschutzbeauftragter bei seiner Tätigkeit Kenntnis von Daten, für die einer der Kontrolle des Datenschutzbeauftragten unterliegenden Stelle beschäftigten Person ein gesetzliches Aussageverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den für

ihn tätigen Personen insoweit zu, als die Person, der das gesetzliche Aussageverweigerungsrecht zusteht, davon Gebrauch gemacht hat. Im Umfang des Aussageverweigerungsrechts des Datenschutzbeauftragten unterliegen seine Akten und andere Schriftstücke einem Sicherstellungs- und Beschlagnahmeverbot.

(3) Der Datenschutzbeauftragte im öffentlichen Bereich (in Formen des öffentlichen Rechts eingerichtet, insbesondere auch als Organ einer Gebietskörperschaft) ist bezüglich der Ausübung seiner Aufgaben weisungsfrei. Das oberste Organ hat das Recht, sich über die Gegenstände der Geschäftsführung beim Datenschutzbeauftragten im öffentlichen Bereich zu unterrichten. Dem ist vom Datenschutzbeauftragten nur insoweit zu entsprechen, als dies nicht der Unabhängigkeit des Datenschutzbeauftragten im Sinne von Art. 38 Abs. 3 DSGVO widerspricht.

(4) Im Wirkungsbereich jedes Bundesministeriums sind unter Bedachtnahme auf Art und Umfang der Datenverarbeitungen sowie je nach Einrichtung des Bundesministeriums ein oder mehrere Datenschutzbeauftragte vorzusehen. Diese müssen dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören.

(5) Die Datenschutzbeauftragten im öffentlichen Bereich gemäß Abs. 4 pflegen einen regelmäßigen Erfahrungsaustausch, insbesondere im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards.

Datengeheimnis

§ 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

2. Abschnitt

Datenverarbeitungen zu spezifischen Zwecken

Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke

§ 7. (1) Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Verantwortliche alle personenbezogenen Daten verarbeiten, die

1. öffentlich zugänglich sind,
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn pseudonymisierte personenbezogene Daten sind und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann.

(2) Bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die nicht unter Abs. 1 fallen, dürfen personenbezogene Daten nur

1. gemäß besonderen gesetzlichen Vorschriften,
2. mit Einwilligung der betroffenen Person oder
3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3

verarbeitet werden.

(3) Eine Genehmigung der Datenschutzbehörde für die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist auf Antrag des Verantwortlichen der Untersuchung zu erteilen, wenn

1. die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet,
2. ein öffentliches Interesse an der beantragten Verarbeitung besteht und
3. die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird.

Sollen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die personenbezogenen Daten beim Verantwortlichen der Untersuchung nur von Personen verarbeitet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Person notwendig ist.

(4) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzuschließen, dass er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(5) Auch in jenen Fällen, in welchen die Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit personenbezogenen Daten gemäß Abs. 1 Z 3 das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

(6) Rechtliche Beschränkungen der Zulässigkeit der Benützung von personenbezogenen Daten aus anderen, insbesondere urheberrechtlichen Gründen, bleiben unberührt.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

§ 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

(2) Wenn allerdings eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung unwahrscheinlich ist, bedarf es keiner Einwilligung, wenn

1. Daten desselben Verantwortlichen verarbeitet werden oder
2. bei einer beabsichtigten Übermittlung der Adressdaten an Dritte
   a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
   b) keine der betroffenen Personen nach entsprechender Information über Anlass und Inhalt der Übermittlung innerhalb angemessener Frist Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Einwilligung der betroffenen Personen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adressdaten mit Genehmigung der Datenschutzbehörde gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse der betroffenen Personen selbst,

2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der betroffenen Personen für wissenschaftliche oder statistische Zwecke

erfolgen soll.

(4) Die Datenschutzbehörde hat auf Antrag eines Verantwortlichen, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der betroffenen Personen der Übermittlung nicht entgegenstehen. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist.

(5) Die übermittelten Adressdaten dürfen ausschließlich für den genehmigten Zweck verarbeitet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) Sofern es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adressdaten notwendigen Verarbeitungen vorgenommen werden.

Freiheit der Meinungsäußerung und Informationsfreiheit

§ 9. (1) Für die Verarbeitung personenbezogener Daten durch Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes – MedienG, BGBl. Nr. 314/1981, sowie durch sonstige Personen, die in einem Medienunternehmen oder Mediendienst auf Grundlage eines Vertrages an der inhaltlichen Gestaltung eines Mediums oder der inhaltlichen Gestaltung der Mitteilungen eines Mediendienstes journalistisch mitwirken, zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes gelten die Bestimmungen der DSGVO sowie dieses Bundesgesetzes mit folgenden Maßgaben:

1. Der Verantwortliche ist gegenüber der betroffenen Person nicht zur Offenlegung von Informationen verpflichtet, die dem Schutz des Redaktionsgeheimnisses (§ 31 MedienG) unterliegen (datenschutzrechtliches Redaktionsgeheimnis); § 31 Abs. 2 MedienG ist anzuwenden. In Verfahren vor Gerichten und Behörden, die Angelegenheiten des Datenschutzes zum Gegenstand haben, gilt § 31 MedienG mit der Maßgabe, dass der Verantwortliche die Beantwortung von Fragen im Sinne des § 31 Abs. 1 MedienG nicht nur als Zeuge, sondern auch als sonst Verfahrensbeteiligter verweigern darf. § 321 Abs. 1 der Zivilprozessordnung – ZPO, RGBl. Nr. 113/1895, ist sinngemäß anzuwenden. Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse den Schutz des Redaktionsgeheimnisses zu beachten.
2. Der Verantwortliche ist berechtigt, personenbezogene Daten einschließlich der in Art. 9 Abs. 1 DSGVO genannten besonderen Kategorien personenbezogener Daten sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (Art. 10 DSGVO) zu verarbeiten, soweit dies für journalistische Zwecke erfolgt. Art. 10 letzter Satz DSGVO bleibt unberührt. Die §§ 12 und 13 dieses Bundesgesetzes sind nicht anwendbar.
3. Art. 5 Abs. 1 lit. a DSGVO gilt in Bezug auf den Grundsatz der Transparenz mit der Maßgabe, dass die Verarbeitung personenbezogener Daten für die betroffene Person nur insoweit nachvollziehbar sein muss, als dadurch die Meinungsäußerungs- und Informationsfreiheit nicht unverhältnismäßig beeinträchtigt wird, und nur insoweit, als die Bestimmungen dieses Absatzes nicht anderes vorsehen.
4. Die Art. 13 und 14 (Informationspflicht) sowie Art. 21 Abs. 1 (Widerspruchsrecht) DSGVO sind nicht anwendbar.
5. Das Auskunftsrecht (Art. 15 DSGVO) ist in Bezug auf personenbezogene Daten, auf deren Grundlage noch keine Veröffentlichung erfolgt ist, nicht anwendbar. Im Übrigen gilt das Auskunftsrecht (Art. 15 DSGVO) mit der Maßgabe, dass die betroffene Person Auskünfte nur in Bezug auf bestimmte, im Antrag auf Auskunft konkret zu bezeichnende Veröffentlichungen verlangen darf und ihre Betroffenheit individuell zu begründen hat und der Verantwortliche abweichend von Art. 12 Abs. 5 erster Satz DSGVO berechtigt ist, für die Bearbeitung von Auskunftsersuchen ein Entgelt von 9 Euro zu verlangen; unterlässt die betroffene Person die konkrete Bezeichnung einer Veröffentlichung, die individuelle Begründung ihrer Betroffenheit oder legt sie keinen Nachweis für die Bezahlung des Entgelts vor, so kann der Verantwortliche sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche ist berechtigt, die Auskunft zu verweigern, soweit dies im Einzelfall zum Schutz der Meinungsäußerungs- und Informationsfreiheit erforderlich und verhältnismäßig ist; in solchen Fällen muss der

Verantwortliche bei der Beantwortung des Auskunftsersuchens gegenüber der betroffenen Person nicht offenlegen, ob ihre personenbezogenen Daten verarbeitet werden, soweit dadurch der Zweck der Auskunftsverweigerung unterlaufen würde. Das Recht auf Kopie (Art. 15 Abs. 3 DSGVO) ist ausgeschlossen.

6. Art. 16 (Recht auf Berichtigung), Art. 17 (Recht auf Löschung) und Art. 18 (Recht auf Einschränkung der Verarbeitung) DSGVO sind nicht anzuwenden
   a) in Bezug auf personenbezogene Daten, auf deren Grundlage noch keine Veröffentlichung erfolgt ist;
   b) in Bezug auf personenbezogene Daten, die in einem Medium im Sinne des § 1 Abs. 1 Z 1 MedienG veröffentlicht wurden;
   c) soweit eine konkurrierende Anspruchsgrundlage wegen Verletzung der Persönlichkeitsrechte der betroffenen Person nach bürgerlichem Recht, insbesondere nach § 20 oder § 1330 des Allgemeinen bürgerlichen Gesetzbuches, JGS Nr. 946/1811, oder nach § 78 des Urheberrechtsgesetzes, BGBl. I Nr. 111/1936, besteht.

   In allen anderen Fällen ist der Verantwortliche im Falle einer Geltendmachung der in Art. 16 und 18 DSGVO genannten Rechte durch die betroffene Person berechtigt, die Berichtigung oder die Einschränkung der Verarbeitung zu verweigern, soweit dies im Einzelfall zum Schutz der Meinungsäußerungs- und Informationsfreiheit erforderlich und verhältnismäßig ist.
7. In den Fällen der Z 5 zweiter und dritter Satz, Z 6 zweiter Satz und Art. 17 Abs. 3 DSGVO ist die betroffene Person berechtigt, eine Überprüfung der Rechtmäßigkeit der Verweigerung der Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung durch die Datenschutzbehörde zu verlangen. Der Verantwortliche hat die betroffene Person über dieses Recht zu unterrichten. Wird dieses Recht ausgeübt, hat der Verantwortliche das Vorliegen der Voraussetzungen der bezüglichen Einschränkung glaubhaft zu machen. § 25 Abs. 3 ist mit der Maßgabe anzuwenden, dass die Datenschutzbehörde die betroffene Person nur darüber zu unterrichten hat, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Datenschutzbehörde erfolgt sind, es sei denn, dass die Datenschutzbehörde zum Ergebnis gelangt, dass die betreffende Einschränkung unzulässig war. Die Datenschutzbehörde hat zudem die betroffene Person über ihr Recht zu unterrichten, Beschwerde an das Bundesverwaltungsgericht zu erheben.
8. Zum Schutz des datenschutzrechtlichen Redaktionsgeheimnisses, sowie soweit dies sonst zum Schutz der Meinungsäußerungs- und Informationsfreiheit, insbesondere im Hinblick auf Z 4 sowie Einschränkungen nach Z 5, erforderlich und verhältnismäßig ist, sind Verantwortliche im Sinne des Abs. 1 erster Satz sowie weitere Verantwortliche, die gemeinsam mit diesen personenbezogene Daten zu den in Abs. 1 erster Satz genannten Zwecken verarbeiten, nicht zur Offenlegung gemäß Art. 26 Abs. 2 zweiter Satz DSGVO verpflichtet.
9. Art. 33 DSGVO (Meldung einer Datenschutzverletzung an die Aufsichtsbehörde) ist mit der Maßgabe anzuwenden, dass eine Verletzung des Schutzes personenbezogener Daten nur dann an die Datenschutzbehörde zu melden ist, wenn sie voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Eine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gemäß Art. 34 DSGVO ist nur nach Maßgabe einer Anweisung der Datenschutzbehörde gemäß Art. 58 Abs. 2 lit. e DSGVO und, soweit das datenschutzrechtliche Redaktionsgeheimnis dadurch nicht beeinträchtigt wird, erforderlich.
10. Art. 38 DSGVO (Stellung des Datenschutzbeauftragten) gilt mit der Maßgabe, dass der Verantwortliche oder der Auftragsverarbeiter den Zugang des Datenschutzbeauftragten zu personenbezogenen Daten, die zu journalistischen Zwecken verarbeitet werden, einschränken kann, soweit dies zum Schutz der Meinungsäußerungs- und Informationsfreiheit erforderlich und verhältnismäßig ist.
11. Der Verantwortliche und der Auftragsverarbeiter sind nicht zur Einhaltung der Vorschriften des Kapitel V der DSGVO (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen) verpflichtet. Unbeschadet des Art. 24 DSGVO (Verantwortung des für die Verarbeitung Verantwortlichen) haben der Verantwortliche und der Auftragsverarbeiter geeignete Maßnahmen zu treffen, um sicherzustellen, dass die Rechte und Freiheiten der betroffenen Person im Falle einer Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nicht unverhältnismäßig beeinträchtigt werden.
12. In Verhaltensregeln gemäß Art. 40 Abs. 2 DSGVO können Einschränkungen gemäß Z 5 dritter Satz und Z 6 zweiter Satz sowie geeignete Maßnahmen im Sinne der Z 11 zweiter Satz dieses Absatzes näher präzisiert werden. Die Datenschutzbehörde hat in Verfahren gemäß Art. 40

Abs. 5 DSGVO eine Stellungnahme der Kommunikationsbehörde Austria („KommAustria“) (§ 1 Abs. 1 KommAustriaG – KOG, BGBl. I Nr. 32/2001) zum Entwurf der Verhaltensregeln bzw. zum Entwurf zu deren Änderung oder Erweiterung einzuholen.

13. Art. 56 (Zuständigkeit der federführenden Aufsichtsbehörde) und Kapitel VII der DSGVO (Zusammenarbeit und Kohärenz) sind nicht anwendbar.

(1a) Für die nicht von Abs. 1 erfasste Verarbeitung personenbezogener Daten zu journalistischen Zwecken gilt Abs. 1 Z 1, 4 und 13; Abs. 1 Z 3 gilt mit der Maßgabe, dass sich der Verweis auf die Bestimmungen in Abs. 1 Z 1, 4 und 13 und Abs. 1a bezieht. Der Verantwortliche ist berechtigt, personenbezogene Daten, aus denen politische Meinungen oder religiöse oder weltanschauliche Überzeugungen hervorgehen (Art. 9 Abs. 1 DSGVO), sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (Art. 10 DSGVO) zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) zu verarbeiten, soweit dies zur Ausübung der Meinungsäußerungs- und Informationsfreiheit erforderlich und verhältnismäßig ist. Art. 10 letzter Satz DSGVO bleibt unberührt. In Bezug auf personenbezogene Daten, die in einem Medium im Sinne des § 1 Abs. 1 Z 1 MedienG veröffentlicht wurden, sind die Art. 16 (Recht auf Berichtigung), 17 (Recht auf Löschung) und 18 (Recht auf Einschränkung der Verarbeitung) DSGVO nicht anzuwenden. Im Übrigen ist der Verantwortliche berechtigt, in Bezug auf zu journalistischen Zwecken verarbeitete personenbezogene Daten, auf deren Grundlage noch keine Veröffentlichung erfolgt ist, im Falle einer Geltendmachung der in den Art. 15 bis 18 DSGVO genannten Rechte durch die betroffene Person die Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung zu verweigern, soweit dies im Einzelfall zum Schutz der Meinungsäußerungs- und Informationsfreiheit erforderlich und verhältnismäßig ist; § 25 Abs. 3 ist anzuwenden. Derartige Einschränkungen können in Verhaltensregeln gemäß Art. 40 Abs. 2 DSGVO näher präzisiert werden. Die Datenschutzbehörde hat in Verfahren gemäß Art. 40 Abs. 5 DSGVO eine Stellungnahme der KommAustria zum Entwurf der Verhaltensregeln bzw. zum Entwurf zu deren Änderung oder Erweiterung einzuholen.

(2) Soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO die Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen § 6 (Datengeheimnis) anzuwenden.

Verarbeitung personenbezogener Daten im Katastrophenfall

§ 10. (1) Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen sind im Katastrophenfall ermächtigt, personenbezogene Daten gemeinsam zu verarbeiten, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist.

(2) Wer rechtmäßig über personenbezogene Daten verfügt, darf diese an Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen übermitteln, sofern diese die personenbezogenen Daten zur Bewältigung der Katastrophe für die in Abs. 1 genannten Zwecke benötigen.

(3) Eine Übermittlung von personenbezogenen Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke unbedingt notwendig ist. Daten, die für sich allein die betroffene Person strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Datenschutzbehörde ist von den veranlassten Übermittlungen und den näheren Umständen des Anlass gebenden Sachverhaltes unverzüglich zu verständigen. Die Datenschutzbehörde hat zum Schutz der Betroffenenrechte weitere Datenübermittlungen zu untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

(4) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Verantwortliche ermächtigt, dem Anfragenden personenbezogene Daten zum Aufenthalt der betroffenen Person und dem Stand der Ausforschung zu übermitteln, wenn der Angehörige seine Identität und das Naheverhältnis glaubhaft darlegt. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) dürfen an nahe Angehörige nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Übermittlung zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger

und Behörden sind verpflichtet, die Verantwortlichen des öffentlichen Bereichs und Hilfsorganisationen zu unterstützen, soweit dies zur Überprüfung der Angaben des Anfragenden erforderlich ist.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der betroffenen Personen zu verstehen. Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Die zu Zwecken der Bewältigung des Katastrophenfalles verarbeiteten personenbezogenen Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

Verwarnung durch die Datenschutzbehörde

§ 11. Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.

3. Abschnitt
Bildverarbeitung

Zulässigkeit der Bildaufnahme

§ 12. (1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn

1. sie im lebenswichtigen Interesse einer Person erforderlich ist,
2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
4. im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn

1. sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,
2. sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist, oder
3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

(4) Unzulässig ist

1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,
2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,
3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten ohne ausdrückliche Einwilligung und für das Erstellen von Persönlichkeitsprofilen mit anderen personenbezogenen Daten oder
4. die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

(5) Im Wege einer zulässigen Bildaufnahme ermittelte personenbezogene Daten dürfen im erforderlichen Ausmaß übermittelt werden, wenn für die Übermittlung eine der Voraussetzungen des Abs. 2 Z 1 bis 4 gegeben ist. Abs. 4 gilt sinngemäß.

Besondere Datensicherheitsmaßnahmen und Kennzeichnung

§ 13. (1) Der Verantwortliche hat dem Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 12 Abs. 3 Z 3.

(5) Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

(6) Die Kennzeichnungspflicht gilt nicht in den Fällen des § 12 Abs. 3 Z 3 und für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer verdeckten Ermittlung erreicht werden kann, unter der Bedingung, dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

(7) Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

2. Hauptstück
Organe

1. Abschnitt
Datenschutzrat

Einrichtung und Aufgaben

§ 14. (1) Beim Bundesministerium für Justiz ist ein Datenschutzrat eingerichtet. Dieser nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben.

(2) Zur Erfüllung seiner Aufgaben nach Abs. 1

1. kann der Datenschutzrat Empfehlungen in datenschutzrechtlicher Hinsicht an die Bundesregierung und die Bundesminister richten;
2. kann der Datenschutzrat Gutachten erstellen oder in Auftrag geben;
3. ist dem Datenschutzrat 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;
4. hat der Datenschutzrat das Recht, von Verantwortlichen des öffentlichen Bereichs Auskünfte und Berichte zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
5. kann der Datenschutzrat seine Beobachtungen, Bedenken und Anregungen veröffentlichen und den Verantwortlichen des öffentlichen Bereichs zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung

§ 15. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Zwölf Mitglieder entsenden die politischen Parteien nach dem System von d'Hondt im Verhältnis ihrer Mandatsstärke im Hauptausschuss des Nationalrates. Jede im Hauptausschuss des Nationalrates vertretene politische Partei hat Anspruch, im Datenschutzrat vertreten zu sein. Eine im Hauptausschuss des Nationalrates vertretene Partei, der nach der obigen Berechnung kein Mitglied zukommt, kann ein Mitglied namhaft machen;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein von der Bundesministerin für Justiz zu entsendender Vertreter des Bundes;
6. ein von der Bundesregierung zu entsendender Vertreter aus dem Kreis der Datenschutzbeauftragten der Bundesministerien;
7. zwei vom Datenschutzrat nach seiner Konstituierung zu benennende nationale oder internationale Experten aus dem Bereich des Datenschutzes.

(2) Die in Abs. 1 genannten Vertreter sollen Kenntnisse sowie Erfahrungen auf den Gebieten des Datenschutzrechtes, des Unionsrechtes und der Grundrechte haben.

(3) Für jedes Mitglied gemäß Abs. 1 Z 1 bis 6 ist ein Ersatzmitglied zu entsenden, welches bei Verhinderung des Mitgliedes an dessen Stelle tritt. Die Entsendung der Mitglieder und Ersatzmitglieder ist dem Bundesministerium für Justiz schriftlich mitzuteilen.

(4) Nicht angehören können dem Datenschutzrat Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind.

(5) Die Funktionsperiode der Mitglieder und Ersatzmitglieder gemäß Abs. 1 Z 1 bis 6 beginnt mit deren Entsendung in den Datenschutzrat und endet

1. mit der Abberufung durch die entsendende Stelle (Abs. 1) im Wege einer schriftlichen Mitteilung an das Bundesministerium für Justiz unter gleichzeitiger Namhaftmachung eines neuen Mitgliedes oder Ersatzmitgliedes,
2. mit der Bekanntgabe des Ausscheidens durch das Mitglied oder Ersatzmitglied im Wege einer schriftlichen Mitteilung an das Bundesministerium für Justiz oder
3. spätestens mit der Neuwahl des Hauptausschusses des Nationalrates nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410/1975.

Auf gemäß Abs. 1 Z 7 benannte Mitglieder des Datenschutzrates findet Z 3 Anwendung.

(6) Nach Neuwahl des Hauptausschusses des Nationalrates (Abs. 5 Z 3) führt das bisherige Präsidium gemäß § 17 Abs. 4 die Geschäfte bis zur konstituierenden Sitzung der neubestellten Mitglieder und Ersatzmitglieder fort. Binnen eines Zeitraumes von zwei Wochen ab der Neuwahl des Hauptausschusses des Nationalrates haben die entsendenden Stellen eine dem Abs. 1 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern dem Bundesministerium für Justiz schriftlich bekannt zu geben. Die Wiederbestellung von Mitgliedern und Ersatzmitgliedern ist zulässig.

(7) Die konstituierende Sitzung des Datenschutzrates hat spätestens sechs Wochen nach der Wahl des Hauptausschusses des Nationalrates stattzufinden und ist vom Bundesministerium für Justiz einzuberufen.

(8) Die Tätigkeit der Mitglieder und Ersatzmitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder und Ersatzmitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der angemessenen Reisekosten nach Maßgabe der Reisegebührenvorschriften des Bundes. Die Vergütungen und Erstattungen sind im Nachhinein quartalsweise vom Bundesministerium für Justiz anzuweisen.

Vorsitz und Geschäftsführung

§ 16. (1) Der Datenschutzrat gibt sich mit Beschluss eine Geschäftsordnung.

(2) Der Datenschutzrat hat in der konstituierenden Sitzung aus den vorliegenden Wahlvorschlägen mit einfacher Mehrheit aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Stichwahlen sind zulässig. Die Wahlvorschläge sind den Mitgliedern und Ersatzmitgliedern gleichzeitig mit der Einladung zur konstituierenden Sitzung bekannt zu geben. Die Wiederwahl ist zulässig.

(3) Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden endet

1. mit Eintritt einer der Voraussetzungen des § 15 Abs. 5 Z 1 bis 3,

2. mit Bekanntgabe der Zurücklegung der Funktion durch den Vorsitzenden oder einen der stellvertretenden Vorsitzenden im Wege einer Erklärung in der Sitzung des Datenschutzrates oder einer schriftlichen Mitteilung an das Bundesministerium für Justiz oder
3. nach Abwahl durch den Datenschutzrat mit einfacher Mehrheit der abgegebenen Stimmen und Anwesenheit von mehr als zwei Drittel seiner Mitglieder oder Ersatzmitglieder.

Nach dem Ende der Funktionsperiode des Vorsitzenden oder eines stellvertretenden Vorsitzenden ist umgehend ein neuer Vorsitzender oder ein neuer stellvertretender Vorsitzender zu wählen.

(4) Der gemäß Abs. 2 gewählte Vorsitzende vertritt den Datenschutzrat nach außen.

(5) Die Geschäftsführung des Datenschutzrates obliegt dem Bundesministerium für Justiz. Die Bundesministerin für Justiz hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundesministeriums für Justiz fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlussfassung

§ 17. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Jedes Mitglied des Datenschutzrates kann schriftlich die Einberufung des Datenschutzrates unter Angabe des gewünschten Verhandlungsgegenstandes begehren. Liegt ein solches Begehren vor, so hat der Vorsitzende die Sitzung so anzuberaumen, dass sie spätestens vier Wochen nach Einlangen des Begehrens stattfindet.

(2) Jedes Mitglied des Datenschutzrates ist – außer im Fall der gerechtfertigten Verhinderung – verpflichtet, an den Sitzungen des Datenschutzrates teilzunehmen. Nur bei Verhinderung des Mitglieds nimmt das Ersatzmitglied an der Sitzung teil.

(3) Für Beratungen und Beschlussfassung im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder oder Ersatzmitglieder erforderlich. Zur Beschlussfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Minderheitenvoten sind zulässig.

(4) Bei dringlichen Angelegenheiten kann der Vorsitzende die stellvertretenden Vorsitzenden und je einen Vertreter der politischen Parteien (§ 15 Abs. 1 Z 1) zu einer außerordentlichen Sitzung (Präsidium) einladen.

(5) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen.

(6) Der Leiter der Datenschutzbehörde und der Vorsitzende des Parlamentarischen Datenschutzkomitees sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen nicht zu.

(7) Der Vorsitzende kann bei Bedarf Sachverständige zu den Sitzungen des Datenschutzrates oder zu Arbeitsausschüssen beiziehen. Auch zur Vorbereitung von Sitzungen des Datenschutzrates oder Arbeitsausschüssen kann der Vorsitzende des Datenschutzrates Experten des jeweiligen Fachgebietes beiziehen, soweit dies zur Klärung von Fragen von besonderer Bedeutung für den Datenschutz erforderlich ist.

(8) Die Beratungen in den Sitzungen des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, nicht öffentlich. Die Mitglieder und Ersatzmitglieder des Datenschutzrates, der Leiter der Datenschutzbehörde sowie sein Stellvertreter, der Vorsitzende des Parlamentarischen Datenschutzkomitees und die zur Sitzung zugezogenen Sachverständigen sind zur Geheimhaltung über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet.

2. Abschnitt
Datenschutzbehörde

Einrichtung

§ 18. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet.

(2) Der Datenschutzbehörde steht ein Leiter vor. In seiner Abwesenheit leitet sein Stellvertreter die Datenschutzbehörde. Auf ihn finden die Regelungen hinsichtlich des Leiters der Datenschutzbehörde Anwendung.

Unabhängigkeit

§ 19. (1) Die Datenschutzbehörde ist eine Dienstbehörde und Personalstelle.

(2) Der Leiter darf für die Dauer seines Amtes keine Tätigkeit ausüben, die

1. Zweifel an der unabhängigen Ausübung seines Amtes oder seiner Unbefangenheit hervorrufen könnte,
2. ihn bei der Erfüllung seiner dienstlichen Aufgaben behindert oder
3. wesentliche dienstliche Interessen gefährdet.

Er ist verpflichtet, Tätigkeiten, die er neben seiner Tätigkeit als Leiter der Datenschutzbehörde ausübt, unverzüglich der Bundesministerin für Justiz zur Kenntnis zu bringen.

(3) Die Bundesministerin für Justiz kann sich beim Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Leiter der Datenschutzbehörde nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Aufsichtsbehörde im Sinne von Art. 52 DSGVO widerspricht.

Leiter der Datenschutzbehörde

§ 20. (1) Der Leiter der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt; die Wiederbestellung ist zulässig. Dem Vorschlag hat eine Ausschreibung zur allgemeinen Bewerbung voranzugehen.

(2) Der Leiter der Datenschutzbehörde hat

1. das Studium der Rechtswissenschaften abgeschlossen zu haben,
2. die persönliche und fachliche Eignung durch eine entsprechende Vorbildung und einschlägige Berufserfahrung in den von der Datenschutzbehörde zu besorgenden Angelegenheiten aufzuweisen,
3. über ausgezeichnete Kenntnisse des österreichischen Datenschutzrechtes, des Unionsrechtes und der Grundrechte zu verfügen und
4. über eine mindestens fünfjährige juristische Berufserfahrung zu verfügen.

(3) Zum Leiter der Datenschutzbehörde dürfen nicht bestellt werden:

1. Mitglieder der Bundesregierung, Staatssekretäre, Mitglieder einer Landesregierung, Mitglieder des Nationalrates, des Bundesrates oder sonst eines allgemeinen Vertretungskörpers oder des Europäischen Parlaments, ferner Volksanwälte und der Präsident des Rechnungshofes,
2. Personen, die eine in Z 1 genannte Funktion innerhalb der letzten zwei Jahre ausgeübt haben, und
3. Personen, die von der Wählbarkeit in den Nationalrat ausgeschlossen sind.

(4) Die Enthebung des Leiters ist auf Vorschlag der Bundesregierung durch den Bundespräsidenten vorzunehmen.

(5) Der Stellvertreter des Leiters der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Maßgabe der Abs. 1 bis 3 bestellt. Auf die Enthebung des Stellvertreters findet Abs. 4 Anwendung.

Aufgaben

§ 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

(2) Die Datenschutzbehörde hat die Listen nach Art. 35 Abs. 4 und 5 DSGVO im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

(3) Die Datenschutzbehörde hat die nach Art. 57 Abs. 1 lit. p DSGVO festzulegenden Kriterien im Wege einer Verordnung kundzumachen. Sie fungiert zugleich als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.

Befugnisse

§ 22. (1) Die Datenschutzbehörde kann vom Verantwortlichen oder Auftragsverarbeiter der überprüften Datenverarbeitung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenverarbeitungen und diesbezügliche Unterlagen begehren. Der Verantwortliche oder

Auftragsverarbeiter hat die notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Verantwortlichen oder des Auftragsverarbeiters und Dritter auszuüben.

(2) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Verantwortlichen oder des Auftragsverarbeiters berechtigt, Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen.

(3) Informationen, die der Datenschutzbehörde oder den von ihr Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Geheimhaltung gilt soweit und solange dies aus den in § 6 Abs. 1 des Informationsfreiheitsgesetzes – IFG, BGBl. I Nr. 5/2024, genannten Gründen erforderlich und verhältnismäßig ist. Im Übrigen besteht die Pflicht zur Geheimhaltung auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach § 63 dieses Bundesgesetzes oder nach §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozeßordnung – StPO, BGBl. Nr. 631/1975, zu entsprechen ist.

(4) Liegt durch den Betrieb einer Datenverarbeitung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51/1991, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen.

(5) Der Datenschutzbehörde obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen.

(6) Bestehen im Zuge einer auf § 29 gestützten Klage einer betroffenen Person, die sich von einer Einrichtung, Organisation oder Vereinigung im Sinne des Art. 80 Abs. 1 DSGVO vertreten lässt, Zweifel am Vorliegen der diesbezüglichen Kriterien, trifft die Datenschutzbehörde auf Antrag des Einbringungsgerichtes entsprechende Feststellungen mit Bescheid. Diese Einrichtung, Organisation oder Vereinigung hat im Verfahren Parteistellung. Gegen einen negativen Feststellungsbescheid steht ihr die Beschwerde an das Bundesverwaltungsgericht offen.

Tätigkeitsbericht und Veröffentlichung von Entscheidungen

§ 23. (1) Die Datenschutzbehörde hat bis zum 31. März eines jeden Jahres einen dem Art. 59 DSGVO entsprechenden Tätigkeitsbericht zu erstellen und der Bundesministerin für Justiz vorzulegen. Der Bericht ist von der Bundesministerin für Justiz der Bundesregierung, dem Nationalrat und dem Bundesrat vorzulegen. Die Datenschutzbehörde hat den Bericht der Öffentlichkeit, der Europäischen Kommission, dem Europäischen Datenschutzausschuss (Art. 68 DSGVO) und dem Datenschutzrat zugänglich zu machen.

(2) Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzbehörde unter Beachtung der Geheimhaltungsgründe gemäß § 6 Abs. 1 IFG in geeigneter Weise zu veröffentlichen.

3. Abschnitt
Rechtsbehelfe, Haftung und Sanktionen

Beschwerde an die Datenschutzbehörde

§ 24. (1) Jede betroffene Person hat das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück verstößt. Dies gilt nicht, soweit ein Recht auf Beschwerde beim Parlamentarischen Datenschutzkomitee gemäß § 35f Abs. 1 besteht.

(2) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(3) Einer Beschwerde sind gegebenenfalls der zu Grunde liegende Antrag und eine allfällige Antwort des Beschwerdegegners anzuschließen. Die Datenschutzbehörde hat im Falle einer Beschwerde auf Ersuchen der betroffenen Person weitere Unterstützung zu leisten.

(4) Der Anspruch auf Behandlung einer Beschwerde erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt. Verspätete Beschwerden sind zurückzuweisen.

(5) Soweit sich eine Beschwerde als berechtigt erweist, ist ihr Folge zu geben. Ist eine Verletzung einem Verantwortlichen des privaten Bereichs zuzurechnen, so ist diesem aufzutragen, den Anträgen des Beschwerdeführers auf Auskunft, Berichtigung, Löschung, Einschränkung oder Datenübertragung in jenem Umfang zu entsprechen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(6) Ein Beschwerdegegner kann bis zum Abschluss des Verfahrens vor der Datenschutzbehörde die behauptete Rechtsverletzung nachträglich beseitigen, indem er den Anträgen des Beschwerdeführers entspricht. Erscheint der Datenschutzbehörde die Beschwerde insofern als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzbehörde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

(7) Der Beschwerdeführer wird von der Datenschutzbehörde innerhalb von drei Monaten ab Einbringung der Beschwerde über den Stand und das Ergebnis der Ermittlung unterrichtet.

(8) Jede betroffene Person kann das Bundesverwaltungsgericht befassen, wenn die Datenschutzbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat.

(9) Die Datenschutzbehörde kann – soweit erforderlich – Amtssachverständige im Verfahren beiziehen.

(10) In die Entscheidungsfrist gemäß § 73 AVG werden nicht eingerechnet:

1. die Zeit, während deren das Verfahren bis zur rechtskräftigen Entscheidung einer Vorfrage ausgesetzt ist;
2. die Zeit während eines Verfahrens nach Art. 56, 60 und 63 DSGVO.

Begleitende Maßnahmen im Beschwerdeverfahren

§ 25. (1) Macht der Beschwerdeführer im Rahmen einer Beschwerde eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verarbeitung seiner personenbezogenen Daten glaubhaft, kann die Datenschutzbehörde nach § 22 Abs. 4 vorgehen.

(2) Ist in einem Verfahren die Richtigkeit von personenbezogenen Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzbehörde auf Antrag des Beschwerdeführers mit Bescheid gemäß § 57 Abs. 1 AVG anzuordnen.

(3) Beruft sich ein Verantwortlicher gegenüber der Datenschutzbehörde auf eine Beschränkung im Sinne des Art. 23 DSGVO, so hat diese die Rechtmäßigkeit der Anwendung der Beschränkungen zu überprüfen. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten personenbezogenen Daten gegenüber der betroffenen Person nicht gerechtfertigt war, ist die Offenlegung der

personenbezogenen Daten mit Bescheid aufzutragen. Wird dem Bescheid der Datenschutzbehörde binnen acht Wochen nicht entsprochen, so hat die Datenschutzbehörde die Offenlegung der personenbezogenen Daten gegenüber der betroffenen Person selbst vorzunehmen und ihr die verlangte Auskunft zu erteilen oder ihr mitzuteilen, welche personenbezogenen Daten bereits berichtigt oder gelöscht wurden.

(4) Bescheide, mit denen Übermittlungen von personenbezogenen Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen oder tatsächlichen Voraussetzungen für die Erteilung der Genehmigung nicht mehr bestehen.

Verantwortliche des öffentlichen und des privaten Bereichs

§ 26. (1) Unbeschadet des § 5 Abs. 3 sind Verantwortliche des öffentlichen Bereichs alle Verantwortlichen,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.

(3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.

(4) Die dem Abs. 1 nicht unterliegenden Verantwortlichen gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes.

Beschwerde an das Bundesverwaltungsgericht

§ 27. (1) Das Bundesverwaltungsgericht entscheidet durch Senat über Beschwerden gegen Bescheide, wegen der Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 und der Entscheidungspflicht der Datenschutzbehörde.

(2) Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Die fachkundigen Laienrichter werden auf Vorschlag der Wirtschaftskammer Österreich und der Bundeskammer für Arbeiter und Angestellte bestellt. Es sind entsprechende Vorkehrungen zu treffen, dass zeitgerecht eine hinreichende Anzahl von fachkundigen Laienrichtern zur Verfügung steht.

(3) Die fachkundigen Laienrichter müssen eine mindestens fünfjährige einschlägige Berufserfahrung und besondere Kenntnisse des Datenschutzrechtes besitzen.

(4) Der Vorsitzende hat den fachkundigen Laienrichtern alle entscheidungsrelevanten Dokumente unverzüglich zu übermitteln oder, wenn dies untunlich oder zur Wahrung der Vertraulichkeit von Dokumenten unbedingt erforderlich ist, zur Verfügung zu stellen.

(5) Kommt es zu einem Verfahren gegen den Bescheid der Datenschutzbehörde, der eine Stellungnahme oder ein Beschluss des Europäischen Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Datenschutzbehörde diese Stellungnahme oder diesen Beschluss dem Bundesverwaltungsgericht zu.

Vertretung von betroffenen Personen

§ 28. Die betroffene Person hat das Recht, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen.

Haftung und Recht auf Schadenersatz

§ 29. (1) Jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art. 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.

(2) Für Klagen auf Schadenersatz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

Allgemeine Bedingungen für die Verhängung von Geldbußen

§ 30. (1) Die Datenschutzbehörde kann Geldbußen gegen eine juristische Person verhängen, wenn Verstöße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben und eine Führungsposition innerhalb der juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,
2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder
3. einer Kontrollbefugnis innerhalb der juristischen Person

innehaben.

(2) Juristische Personen können wegen Verstößen gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 1 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet.

(3) Die Datenschutzbehörde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(4) Die gemäß § 22 Abs. 5 verhängten Geldbußen fließen dem Bund zu und sind nach den Bestimmungen über die Eintreibung von gerichtlichen Geldstrafen einzubringen. Rechtskräftige Bescheide der Datenschutzbehörde sind Exekutionstitel. Die Bewilligung und der Vollzug der Exekution ist auf Grund des Exekutionstitels der Datenschutzbehörde bei dem Bezirksgericht, in dessen Sprengel der Verpflichtete seinen allgemeinen Gerichtsstand in Streitsachen hat (§§ 66, 75 der Jurisdiktionsnorm – JN, RGBl. Nr. 111/1895), oder bei dem in den §§ 18 und 19 EO bezeichneten Exekutionsgericht zu beantragen.

(5) Gegen Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts können keine Geldbußen verhängt werden.

4. Abschnitt
Aufsichtsbehörde nach der Richtlinie (EU) 2016/680

Datenschutzbehörde

§ 31. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde für den in § 36 Abs. 1 genannten Anwendungsbereich eingerichtet. Die Datenschutzbehörde ist nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

(2) Hinsichtlich der Unabhängigkeit, der allgemeinen Bedingungen und der Errichtung der Aufsichtsbehörde finden die Art. 52, 53 und 54 DSGVO sowie der § 18 Abs. 2, §§ 19 und 20 sinngemäß Anwendung.

Aufgaben der Datenschutzbehörde

§ 32. (1) Die Datenschutzbehörde hat im Anwendungsbereich des § 36 Abs. 1

1. die Anwendung des § 1 und der im 3. Hauptstück erlassenen Vorschriften sowie der Durchführungsvorschriften zur 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, zu überwachen und durchzusetzen;
2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären;
3. die in Art. 57 Abs. 1 lit. c bis e, g, h und t DSGVO festgelegten Aufgaben im Hinblick auf das 3. Hauptstück zu erfüllen;
4. sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder einer Vereinigung gemäß § 28 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer Frist von drei Monaten über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

5. die Rechtmäßigkeit der Verarbeitung gemäß § 42 Abs. 8 zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß § 42 Abs. 9 zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen wurde;
6. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie,
7. Beratung in Bezug auf die in § 53 genannten Verarbeitungsvorgänge zu leisten, und
8. die Rechte der betroffenen Person in den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 auszuüben.

(2) Die Datenschutzbehörde erleichtert das Einreichen von in Abs. 1 Z 4 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Art. 57 Abs. 3 und 4 DSGVO finden sinngemäß Anwendung.

Befugnisse der Datenschutzbehörde

§ 33. (1) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Untersuchungsbefugnisse. Diese umfassen insbesondere die in § 22 Abs. 2 genannten Befugnisse.

(2) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Abhilfebefugnisse. Dazu zählen jedenfalls die Befugnisse, die es ihr gestatten

1. einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften verstoßen;
2. den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß § 45;
3. eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

(3) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung erforderlichen wirksamen Beratungsbefugnisse, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach § 53 den Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an den Nationalrat oder den Bundesrat, die Bundes- oder Landesregierung oder an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

(4) Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse richtet sich im Anwendungsbereich § 36 Abs. 1 sinngemäß nach Art. 58 Abs. 4 DSGVO.

(5) § 22 Abs. 3 2. Satz gilt sinngemäß für Verstöße im Anwendungsbereich des § 36 Abs. 1.

Allgemeine Bestimmungen

§ 34. (1) Verantwortliche haben im Anwendungsbereich des § 36 Abs. 1 wirksame Vorkehrungen zu treffen, um vertrauliche Meldungen über Verstöße zu fördern. In diesem Sinne haben Verantwortliche insbesondere angemessene Verfahren einzurichten, die es ermöglichen, Verstöße gegen die Bestimmungen des 3. Hauptstücks an eine geeignete Stelle zu melden.

(2) Die in Abs. 1 angeführten Vorkehrungen umfassen zumindest

1. spezielle Verfahren für den Empfang der Meldungen über Verstöße und deren Weiterverfolgung;
2. den Schutz personenbezogener Daten sowohl für die Person, die die Verstöße anzeigt, als auch für die natürliche Person, die mutmaßlich für einen Verstoß verantwortlich ist;
3. klare Regeln, welche die Geheimhaltung der Identität der Person, die die Verstöße anzeigt, gewährleisten, soweit nicht die Offenlegung der Identität im Rahmen eines staatsanwaltschaftlichen, gerichtlichen oder verwaltungsrechtlichen Verfahrens zwingend zu erfolgen hat.

(3) Die Datenschutzbehörde hat im Rahmen des Tätigkeitsberichtes nach § 23 über die Tätigkeiten nach dem 4. und 5. Abschnitt zu berichten. Die Vorgaben des Art. 59 DSGVO und § 23 für den Tätigkeitsbericht und die Veröffentlichung von Entscheidungen finden sinngemäß Anwendung.

(4) Auf die gegenseitige Amtshilfe im Anwendungsbereich des § 36 Abs. 1 findet Art. 61 Abs. 1 bis 7 DSGVO sinngemäß Anwendung.

(5) Im Anwendungsbereich des § 36 Abs. 1 finden die Regelungen des 3. Abschnitts des 2. Hauptstücks – mit Ausnahme des § 30 – sinngemäß Anwendung.

5. Abschnitt
Besondere Befugnisse der Datenschutzbehörde

§ 35. (1) Die Datenschutzbehörde ist nach den näheren Bestimmungen der DSGVO und dieses Bundesgesetzes zur Wahrung des Datenschutzes berufen.

(2) **(Verfassungsbestimmung)** Die Datenschutzbehörde übt ihre Befugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung sowie gegenüber dem Präsidenten des Verwaltungsgerichtshofes im Bereich der diesem zustehenden Verwaltungsangelegenheiten aus.

6. Abschnitt
Parlamentarisches Datenschutzkomitee

Einrichtung

§ 35a. (**Verfassungsbestimmung**) (1) Für den Bereich der Gesetzgebung wird das Parlamentarische Datenschutzkomitee als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet. Es ist zuständig für die Aufsicht über die Verarbeitungen

1. des Nationalrates und des Bundesrates einschließlich deren Mitglieder in Ausübung ihres Mandates sowie der Funktionäre gemäß § 56i Abs. 1 Z 1 bis 3 des Verfassungsgerichtshofgesetzes 1953 – VfGG, BGBl. Nr. 85/1953,
2. des Rechnungshofes und der Volksanwaltschaft,
3. der obersten Organe gemäß Art. 30 Abs. 3 bis 6, 125 und 148h Abs. 1 und 2 B-VG im Bereich der diesen zustehenden Verwaltungsangelegenheiten.

(2) Durch Landesverfassungsgesetz kann die Zuständigkeit des Parlamentarischen Datenschutzkomitees für die Aufsicht über die Verarbeitungen der Landtage einschließlich deren Mitglieder in Ausübung ihres Mandates, der Landesrechnungshöfe und der Landesvolksanwälte vorgesehen werden. Dabei kann auch die Zuständigkeit für die Aufsicht über die Verarbeitungen im Bereich der Verwaltungsangelegenheiten der Landtage, der Landesrechnungshöfe und der Landesvolksanwälte vorgesehen werden.

(3) Das Parlamentarische Datenschutzkomitee ist eine Dienstbehörde und Personalstelle. Die Diensthoheit des Bundes gegenüber den beim Parlamentarischen Datenschutzkomitee Bediensteten wird von dessen Vorsitzenden ausgeübt.

Mitglieder

§ 35b. (1) **(Verfassungsbestimmung)** Die Mitglieder des Parlamentarischen Datenschutzkomitees werden auf Vorschlag des Hauptausschusses vom Nationalrat mit Zustimmung des Bundesrates für eine Funktionsperiode von fünf Jahren gewählt; die Wiederwahl ist zulässig. Die Anzahl der Mitglieder hat mindestens drei und höchstens sechs zu betragen. Dem Vorschlag des Hauptausschusses hat eine Ausschreibung zur allgemeinen Bewerbung durch den Präsidenten des Nationalrates voranzugehen. Der Vorschlag des Hauptausschusses, die Wahl durch den Nationalrat und die Zustimmung des Bundesrates bedürfen jeweils der Anwesenheit von mindestens der Hälfte der Mitglieder und einer Mehrheit von zwei Dritteln der abgegebenen Stimmen. Die Mitglieder des Parlamentarischen Datenschutzkomitees leisten vor Antritt ihres Amtes dem Bundespräsidenten die Angelobung.

(2) Die Mitglieder des Parlamentarischen Datenschutzkomitees haben

1. über ein abgeschlossenes Studium zu verfügen, wobei es sich bei mindestens der Hälfte der Mitglieder um ein rechtswissenschaftliches Studium handeln muss,
2. die persönliche und fachliche Eignung durch eine entsprechende Vorbildung und mindestens fünfjährige einschlägige Berufserfahrung aufzuweisen und

3. über Kenntnisse des österreichischen und europäischen Datenschutzrechts, der Grundrechte, des Parlamentsrechts und des parlamentarischen Verfahrens zu verfügen.

(3) Zum Mitglied des Parlamentarischen Datenschutzkomitees dürfen nicht bestellt werden:

1. Mitglieder der Bundesregierung, Staatssekretäre, Mitglieder einer Landesregierung, Mitglieder des Nationalrates, des Bundesrates oder sonst eines allgemeinen Vertretungskörpers oder des Europäischen Parlaments, ferner der Präsident des Rechnungshofes und die Mitglieder der Volksanwaltschaft sowie Direktoren der Landesrechnungshöfe und Landesvolksanwälte,
2. Personen, die eine in Z 1 genannte Funktion innerhalb der letzten fünf Jahre ausgeübt haben, und
3. Personen, die von der Wählbarkeit in den Nationalrat ausgeschlossen sind.

(4) **(Verfassungsbestimmung)** Die Enthebung eines Mitglieds des Parlamentarischen Datenschutzkomitees ist auf Vorschlag des Hauptausschusses durch den Nationalrat vorzunehmen, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt (Art. 53 Abs. 4 DSGVO). Der Vorschlag des Hauptausschusses und der Beschluss des Nationalrates bedürfen jeweils der Anwesenheit von mindestens der Hälfte der Mitglieder und einer Mehrheit von zwei Dritteln der abgegebenen Stimmen.

(5) Den Mitgliedern des Parlamentarischen Datenschutzkomitees gebührt als Entschädigung für die Erfüllung ihrer Aufgaben für jede begonnene Stunde ein Zehntel der Entschädigung eines Ersatzmitgliedes des Verfassungsgerichtshofes für einen Sitzungstag (§ 4 Abs. 3 VfGG). Für die Vergütung ihrer Reisekosten gelten die Bestimmungen der Reisegebührenvorschrift 1955, BGBl. Nr. 133/1955, sinngemäß.

Unabhängigkeit

§ 35c. (1) Die Mitglieder des Parlamentarischen Datenschutzkomitees üben dieses Amt neben ihren beruflichen Tätigkeiten aus. Sie dürfen für die Dauer ihres Amtes lediglich keine Tätigkeit ausüben, die

1. Zweifel an der unabhängigen Ausübung ihres Amtes oder ihrer Unbefangenheit hervorrufen könnte, oder
2. sie bei der Erfüllung ihrer Aufgaben als Mitglied des Parlamentarischen Datenschutzkomitees behindert oder wesentliche Interessen dieser Aufgabe gefährdet.

Sie sind verpflichtet, ihre beruflichen Tätigkeiten, die sie neben ihrer Tätigkeit als Mitglied des Parlamentarischen Datenschutzkomitees ausüben, unverzüglich dem Vorsitzenden des Parlamentarischen Datenschutzkomitees zu melden.

(2) Der Vorsitzende des Parlamentarischen Datenschutzkomitees hat seine und die gemäß Abs. 1 gemeldeten beruflichen Tätigkeiten im Internet zu veröffentlichen. Die Veröffentlichungen sind für die Dauer der jeweiligen Funktionsperiode aufrecht zu erhalten.

(3) **(Verfassungsbestimmung)** Der Präsident des Nationalrates kann sich beim Vorsitzenden des Parlamentarischen Datenschutzkomitees über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Vorsitzenden des Parlamentarischen Datenschutzkomitees nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Aufsichtsbehörde im Sinne von Art. 52 DSGVO widerspricht.

Vorsitz und Beschlussfassung

§ 35d. (1) Der Vorsitz des Parlamentarischen Datenschutzkomitees wechselt jährlich zwischen den Mitgliedern. Die Reihenfolge ist in der Geschäftsordnung festzulegen. Bei Bedarf bestimmt das Parlamentarische Datenschutzkomitee aus seiner Mitte eine Stellvertretung, die ebenfalls jährlich wechselt; der Stellvertreter vertritt den Vorsitzenden des Parlamentarischen Datenschutzkomitees in dessen Abwesenheit. Der Vorsitzende des Parlamentarischen Datenschutzkomitees hat dem Präsidenten des Nationalrates rechtzeitig einen Entwurf betreffend die für die Aufgabenerfüllung des Parlamentarischen Datenschutzkomitees erforderlichen Ressourcen als Grundlage für die Erstellung des Voranschlagsentwurfs gemäß § 14 Abs. 2 des Geschäftsordnungsgesetzes 1975 zu unterbreiten.

(2) Das Parlamentarische Datenschutzkomitee ist bei Anwesenheit von mehr als der Hälfte seiner Mitglieder beschlussfähig. Es fasst seine Beschlüsse mit Stimmenmehrheit. Ein befangenes Mitglied hat sich seiner Stimme zu enthalten; ansonsten ist Stimmenthaltung unzulässig.

(3) Die Sitzungen des Parlamentarischen Datenschutzkomitees können auch als Telefon- oder Videokonferenz (auch in hybrider Form) stattfinden. Mitglieder, die durch Telefon- oder Videokonferenz zugeschaltet sind, gelten als anwesend. Eine Beschlussfassung auf schriftlichem oder elektronischem Weg im Umlaufverfahren ist zulässig. Näheres bestimmt die Geschäftsordnung des Parlamentarischen Datenschutzkomitees.

(4) Das Parlamentarische Datenschutzkomitee hat sich durch Beschluss eine Geschäftsordnung zu geben. Die Geschäftsordnung hat insbesondere Regelungen über die Reihenfolge des Vorsitzes und gegebenenfalls der Stellvertretung sowie über die Arbeitsweise des Parlamentarischen Datenschutzkomitees zu enthalten. In der Geschäftsordnung können einzelne Mitglieder mit der Führung der laufenden Geschäfte und bestimmten verfahrensrechtlichen Angelegenheiten betraut werden. Bis zum Beschluss der Geschäftsordnung lädt das an Jahren älteste Mitglied zur Sitzung ein und leitet diese.

Aufgaben, Befugnisse, Tätigkeitsbericht und Veröffentlichung von Entscheidungen

§ 35e. (1) Genehmigungen gemäß § 7 Abs. 2 Z 3 und Abs. 3 sowie § 8 Abs. 3 und 4, soweit dadurch personenbezogene Daten aus Verarbeitungen gemäß § 35a Abs. 1 betroffen sind, obliegen dem Parlamentarischen Datenschutzkomitee. Dies gilt auch in Bezug auf personenbezogene Daten aus Verarbeitungen gemäß § 35a Abs. 2, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

(2) § 21 Abs. 1, § 22 und § 30 Abs. 5 gelten sinngemäß. Gegenüber den in § 2 des Informationsordnungsgesetzes – InfOG, BGBl. I Nr. 102/2014, genannten Personen bestehen die Untersuchungsbefugnisse gemäß § 22 Abs. 1 und 2 (Art. 58 Abs. 1 lit. e und f DSGVO) jedoch nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungsverpflichtungen dieser Personen führen würde. Gegenüber dem Rechnungshof und der Volksanwaltschaft bestehen die Untersuchungsbefugnisse gemäß § 22 Abs. 1 und 2 (Art. 58 Abs. 1 lit. e und f DSGVO) nicht, soweit die Inanspruchnahme dieser Befugnisse zu einer Verletzung von Geheimhaltungsverpflichtungen des Rechnungshofes oder der Volksanwaltschaft führen würde.

(3) **(Verfassungsbestimmung)** § 23 gilt sinngemäß mit der Maßgabe, dass der Tätigkeitsbericht dem Präsidenten des Nationalrates und von diesem der Bundesregierung, dem Nationalrat, dem Bundesrat und, soweit eine Zuständigkeit des Parlamentarischen Datenschutzkomitees gemäß § 35a Abs. 2 vorgesehen wurde, den Landtagen vorzulegen ist.

Beschwerde an das Parlamentarische Datenschutzkomitee

§ 35f. (1) Jede betroffene Person hat das Recht auf Beschwerde beim Parlamentarischen Datenschutzkomitee, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gemäß § 35a Abs. 1 gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück verstößt. Dies gilt auch in Bezug auf Verarbeitungen gemäß § 35a Abs. 2, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

(2) § 24 Abs. 2 bis 9 und Abs. 10 Z 1 sowie § 28 gelten sinngemäß.

Parteistellung, Rechtsmittellegitimation und Geheimhaltungsverpflichtung

§ 35g. (1) **(Verfassungsbestimmung)** Die für die Verarbeitungen gemäß § 35a Abs. 1 Verantwortlichen sind Partei in Verfahren vor dem Parlamentarischen Datenschutzkomitee. Dasselbe gilt für die für Verarbeitungen gemäß § 35a Abs. 2 Verantwortlichen, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

(2) **(Verfassungsbestimmung)** Die für die Verarbeitungen gemäß § 35a Abs. 1 Verantwortlichen können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben. Dasselbe gilt für die für Verarbeitungen gemäß § 35a Abs. 2 Verantwortlichen, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

(3) Erlangen das Parlamentarische Datenschutzkomitee, das Bundesverwaltungsgericht, der Verwaltungsgerichtshof oder der Verfassungsgerichtshof im Rahmen eines Verfahrens betreffend Verarbeitungen gemäß § 35a Abs. 1 Kenntnis von Informationen, die einer gesetzlichen Geheimhaltungsverpflichtung unterliegen, gilt die Geheimhaltungsverpflichtung auch für diese. Dies gilt auch in Bezug auf Verarbeitungen gemäß § 35a Abs. 2, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

Beschwerde an das Bundesverwaltungsgericht

§ 35h. § 27 Abs. 1 gilt sinngemäß. § 27 Abs. 2 bis 4 kommt nicht zur Anwendung.

7. Abschnitt

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle und Zusammenarbeit der Aufsichtsbehörden in Angelegenheiten der Europäischen Union

Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

§ 35i. Gemeinsamer Vertreter im Europäischen Datenschutzausschuss (Art. 68 DSGVO) und zentrale Anlaufstelle ist der Leiter der Datenschutzbehörde.

Zusammenarbeit und Kohärenz

§ 35j. Die Datenschutzbehörde und das Parlamentarische Datenschutzkomitee arbeiten in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammen. In Bezug auf den Europäischen Datenschutzausschuss (Kapitel VII. der DSGVO) hat die Datenschutzbehörde das Parlamentarische Datenschutzkomitee über alle Angelegenheiten rechtzeitig zu informieren und jedenfalls einzubinden, wenn dieses von der Angelegenheit betroffen sein könnte.

3. Hauptstück

Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des Verfassungsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs

1. Abschnitt

Allgemeine Bestimmungen

Anwendungsbereich und Begriffsbestimmungen

§ 36. (1) Die Bestimmungen dieses Hauptstücks gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, 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.

(2) Im Sinne dieses Hauptstücks bezeichnet der Ausdruck:

1. „personenbezogene Daten“ 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;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
7. „zuständige Behörde“
   a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, die nationale Sicherheit, den Nachrichtendienst oder die militärische Eigensicherung zuständig ist, oder
   b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zum Zweck der nationalen Sicherheit, des Nachrichtendienstes oder der militärischen Eigensicherung übertragen wurde;
8. „Verantwortlicher“ die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
9. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
10. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags aufgrund von Gesetzen möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
11. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
12. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
13. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
14. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
15. „Aufsichtsbehörde“ die Datenschutzbehörde;
16. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Grundsätze für die Datenverarbeitung, Kategorisierung und Datenqualität

§ 37. (1) Personenbezogene Daten

1. müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. müssen dem Verarbeitungszweck entsprechen dafür maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein,
4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,
5. dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,
6. müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder

unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke im Anwendungsbereich des § 36 Abs. 1 gilt § 38.

(3) Der Verantwortliche ist für die Einhaltung der Abs. 1 und 2 verantwortlich und muss deren Einhaltung nachweisen können.

(4) Soweit möglich und zumutbar, ist zwischen den personenbezogenen Daten insbesondere folgender Kategorien betroffener Personen zu unterscheiden:

1. Personen, die aufgrund bestimmter Tatsachen konkret verdächtig sind, eine strafbare Handlung begangen zu haben,
2. Personen, gegen die aufgrund bestimmter Tatsachen der begründete Verdacht besteht, dass sie in naher Zukunft eine strafbare Handlung begehen werden,
3. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer Straftat sind, und
5. sonstige Personen, die im Zusammenhang mit einer Straftat stehen, insbesondere Personen, die als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den in Z 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.

(5) Soweit möglich ist zwischen faktenbasierten und auf persönlichen Einschätzungen beruhenden personenbezogenen Daten zu unterscheiden. Auf persönlichen Einschätzungen beruhende personenbezogene Daten sind entsprechend zu kennzeichnen und können mit einer Begründung versehen werden, welche die Nachvollziehbarkeit der Einschätzung ermöglicht.

(6) Unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten dürfen weder übermittelt noch zum automatisierten Abruf aus Dateisystemen bereitgestellt werden. Die Behörde hat zu diesem Zweck vor einer Übermittlung die Datenqualität soweit möglich entsprechend zu überprüfen. Zum automatisierten Abruf bereit gehaltene personenbezogene Daten sind entsprechend laufend vollständig und aktuell zu halten.

(7) Bei jeder Übermittlung personenbezogener Daten sind soweit möglich die zur Beurteilung der Aktualität, Richtigkeit, Vollständigkeit und Zuverlässigkeit der personenbezogenen Daten durch den Empfänger erforderlichen Informationen beizufügen.

(8) Wird von Amts wegen oder infolge einer Mitteilung eines Betroffenen festgestellt, dass personenbezogene Daten übermittelt worden sind, die nicht den Anforderungen nach Abs. 6 entsprechen, teilt die übermittelnde bzw. dateisystemführende Dienststelle und Behörde dies der empfangenden Stelle oder Behörde unverzüglich mit. Letztere hat unverzüglich die Löschung unrechtmäßig übermittelter Daten, die Berichtigung unrichtiger Daten, die Ergänzung unvollständiger Daten oder eine Einschränkung der Verarbeitung vorzunehmen.

(9) Hat die empfangende Dienststelle oder Behörde Grund zur Annahme, dass übermittelte personenbezogene Daten unrichtig oder nicht aktuell sind oder zu löschen oder in der Verarbeitung einzuschränken wären, so unterrichtet sie die übermittelnde Dienststelle oder Behörde unverzüglich hierüber. Letztere ergreift unverzüglich die erforderlichen Maßnahmen.

Rechtmäßigkeit der Verarbeitung

§ 38. Die Verarbeitung personenbezogener Daten ist, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird.

Verarbeitung besonderer Kategorien personenbezogener Daten

§ 39. Die Verarbeitung personenbezogener Daten, aus denen die rassische oder 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 für die in § 36 Abs. 1 genannten Zwecke ist nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und

1. die Verarbeitung gemäß § 38 zulässig ist oder
2. sie sich auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat.

Verarbeitung für andere Zwecke und Übermittlung

§ 40. (1) Eine Verarbeitung von personenbezogenen Daten nach den Bestimmungen dieses Hauptstücks durch denselben oder einen anderen Verantwortlichen für einen anderen Verarbeitungszweck, als jenen, für den sie erhoben wurden, ist nur zulässig, wenn dieser andere Zweck vom Anwendungsbereich des § 36 Abs. 1 umfasst ist und die Voraussetzungen der §§ 38 und 39 erfüllt sind.

(2) Die Übermittlung von nach den Bestimmungen dieses Hauptstücks verarbeiteten personenbezogenen Daten für einen nicht in § 36 Abs. 1 genannten Zweck ist nur zulässig, wenn dies gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen ist und der Empfänger zur Verarbeitung dieser personenbezogenen Daten für diesen anderen Zweck befugt ist.

(3) Unterliegt die Verarbeitung von personenbezogenen Daten besonderen Bedingungen, so hat die übermittelnde zuständige Behörde den Empfänger der personenbezogenen Daten darauf hinzuweisen, dass diese Bedingungen gelten und einzuhalten sind. Die Übermittlung an Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen darf keinen Bedingungen unterworfen werden, die nicht auch für entsprechende Datenübermittlungen im Inland gelten.

Automatisierte Entscheidungsfindung im Einzelfall

§ 41. (1) Ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen einschließlich Profiling, die für die betroffene Person nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können, sind nur zulässig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen sind.

(2) Entscheidungen nach Abs. 1 dürfen nur auf besonderen Kategorien personenbezogener Daten nach § 39 beruhen, wenn und soweit wirksame Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Entscheidungen nach Abs. 1, die zur Folge haben, dass natürliche Personen auf Grundlage von personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung diskriminiert werden, sind verboten.

2. Abschnitt
Rechte der betroffenen Person

Grundsätze

§ 42. (1) Der Verantwortliche hat der betroffenen Person alle Informationen und Mitteilungen gemäß §§ 43 bis 45, die sich auf die Verarbeitung beziehen, in möglichst präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Informationen sind in geeigneter Form, im Falle eines Antrags nach Möglichkeit in der gleichen Form wie der Antrag, zu übermitteln.

(2) Der Verantwortliche hat den betroffenen Personen die Ausübung der ihnen gemäß §§ 43 bis 45 zustehenden Rechte zu erleichtern.

(3) Der Verantwortliche hat die betroffene Person unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit ihrem Antrag verfahren wurde.

(4) Der Verantwortliche stellt der betroffenen Person Informationen über die aufgrund eines Antrags gemäß §§ 44 bis 45 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(5) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(6) Informationen gemäß § 43 sowie alle Mitteilungen und Maßnahmen gemäß den §§ 44 und 45 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

1. ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
2. sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(7) Der Verantwortliche kann zur Bestätigung der Identität der Person, die einen Antrag gemäß §§ 44 oder 45 gestellt hat, erforderliche zusätzliche Informationen verlangen.

(8) In den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 ist die betroffene Person berechtigt, eine Überprüfung der Rechtmäßigkeit der bezüglichen Einschränkung ihrer Rechte durch die Datenschutzbehörde zu verlangen. Der Verantwortliche hat die betroffene Person über dieses Recht zu unterrichten.

(9) Wird das in Abs. 8 genannte Recht ausgeübt, hat die Datenschutzbehörde die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Datenschutzbehörde erfolgt sind. Die Datenschutzbehörde hat zudem die betroffene Person über ihr Recht zu unterrichten, Beschwerde an das Bundesverwaltungsgericht zu erheben.

Information der betroffenen Person

§ 43. (1) Der Verantwortliche hat der betroffenen Person zumindest die folgenden Informationen zur Verfügung zu stellen:

1. den Namen und die Kontaktdaten des Verantwortlichen,
2. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden,
4. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
5. das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) Zusätzlich zu den in Abs. 1 genannten Informationen hat der Verantwortliche der betroffenen Person in besonderen Fällen die folgenden zusätzlichen Informationen zu erteilen, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:

1. die Rechtsgrundlage der Verarbeitung,
2. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
3. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,
4. erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

(3) Im Fall der Erhebung der personenbezogenen Daten bei der betroffenen Person müssen der betroffenen Person die Informationen nach den Vorgaben des Abs. 1 und 2 zum Zeitpunkt der Erhebung vorliegen. In allen übrigen Fällen findet Art. 14 Abs. 3 DSGVO Anwendung. Die Information gemäß Abs. 1 und 2 kann entfallen, wenn die Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Verantwortlichen oder aus Anwendungen anderer Verantwortlicher ermittelt und die Datenverarbeitung durch Gesetz vorgesehen ist.

(4) Die Unterrichtung der betroffenen Person gemäß Abs. 2 kann soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden, wie dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist

1. zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, insbesondere durch die Behinderung behördlicher oder gerichtlicher Untersuchungen, Ermittlungen oder Verfahren,

2. zum Schutz der öffentlichen Sicherheit,
3. zum Schutz der nationalen Sicherheit,
4. zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,
5. zum Schutz der militärischen Eigensicherung oder
6. zum Schutz der Rechte und Freiheiten anderer.

Auskunftsrecht der betroffenen Person

§ 44. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über personenbezogene Daten und zu folgenden Informationen zu erhalten:

1. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
2. die Kategorien personenbezogener Daten, die verarbeitet werden,
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,
4. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
5. das Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen,
6. das Bestehen eines Beschwerderechts bei der Datenschutzbehörde sowie deren Kontaktdaten und
7. Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.

(2) Einschränkungen des Auskunftsrechts sind nur unter den in § 43 Abs. 4 angeführten Voraussetzungen zulässig.

(3) Im Falle einer Nichterteilung der Auskunft gemäß Abs. 2 hat der Verantwortliche die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür zu unterrichten. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in § 43 Abs. 4 genannten Zwecke zuwiderliefe. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, Beschwerde bei der Datenschutzbehörde einzulegen.

(4) Der Verantwortliche hat die Gründe für die Entscheidung über die Nichterteilung der Auskunft gemäß Abs. 2 zu dokumentieren. Diese Angaben sind der Datenschutzbehörde zur Verfügung zu stellen.

(5) In dem Umfang, in dem eine Datenverarbeitung für eine betroffene Person hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.

Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung

§ 45. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten sowie die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Die Berichtigung oder Vervollständigung kann erforderlichenfalls mittels einer ergänzenden Erklärung erfolgen, soweit eine nachträgliche Änderung mit dem Dokumentationszweck unvereinbar ist. Der Beweis der Richtigkeit der Daten obliegt dem Verantwortlichen, soweit die personenbezogenen Daten nicht ausschließlich aufgrund von Angaben der betroffenen Person ermittelt wurden.

(2) Der Verantwortliche hat personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzüglich zu löschen, wenn

1. die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
2. die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder
3. die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder
2. die personenbezogenen Daten für Beweiszwecke im Rahmen der Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe weiter aufbewahrt werden müssen.

Im Falle einer Einschränkung gemäß Z 1 hat der Verantwortliche die betroffene Person vor einer Aufhebung der Einschränkung zu unterrichten.

(4) Der Verantwortliche hat die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder eine Einschränkung der Verarbeitung und über die Gründe für die Verweigerung zu unterrichten. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, bei der Datenschutzbehörde Beschwerde einzulegen.

(5) Der Verantwortliche hat die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen personenbezogenen Daten stammen, mitzuteilen.

(6) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß Abs. 1 bis 3 hat der Verantwortliche alle Empfänger der betroffenen personenbezogenen Daten in Kenntnis zu setzen. Die Empfänger sind verpflichtet, die ihrer Verantwortung unterliegenden personenbezogenen Daten unverzüglich zu berichtigen, löschen oder deren Verarbeitung einschränken.

(Anm.: Abs. 7 aufgehoben durch Z 22, BGBl. I Nr. 24/2018)

3. Abschnitt
Verantwortlicher und Auftragsverarbeiter

Pflichten des Verantwortlichen

§ 46. Der Verantwortliche hat die in Art. 24 Abs. 1 und 2 sowie Art. 25 Abs. 1 und 2 DSGVO angeführten Verpflichtungen in Bezug auf die Übereinstimmung der Verarbeitung mit den Bestimmungen dieses Hauptstücks einzuhalten.

Gemeinsam Verantwortliche

§ 47. Zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sind gemeinsam Verantwortliche. Sie haben in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben nach diesem Bundesgesetz festzulegen, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß § 43 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich festgelegt sind. In der Vereinbarung ist eine Anlaufstelle für die betroffenen Personen anzugeben.

Auftragsverarbeiter und Aufsicht über die Verarbeitung

§ 48. (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Bundesgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen in Anspruch.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund ausdrücklicher gesetzlicher Ermächtigung, der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag oder dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

1. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Unionsrecht oder durch Gesetze, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung

mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

2. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. alle gemäß § 54 erforderlichen Maßnahmen ergreift;
4. die in den Abs. 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
5. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in diesem Hauptstück genannten Rechte der betroffenen Person nachzukommen;
6. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 52 bis 56 genannten Pflichten unterstützt;
7. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder aufgrund von Gesetzen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
8. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Abs. 1 bis 6 niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Im Hinblick auf Z 8 informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen dieses Hauptstücks oder gegen andere Datenschutzbestimmungen der Union oder gesetzliche Datenschutzbestimmungen verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund von Gesetzen dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Abs. 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieses Hauptstücks erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Der Vertrag oder das andere Rechtsinstrument im Sinne der Abs. 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(6) Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder aufgrund von Gesetzen zur Verarbeitung verpflichtet sind.

(7) Ein Auftragsverarbeiter, der unter Verstoß gegen dieses Hauptstück die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

Verzeichnis von Verarbeitungstätigkeiten

§ 49. (1) Jeder Verantwortliche hat sinngemäß nach Maßgabe des Art. 30 Abs. 1 bis 4 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen, wobei sich die Verweise in Art. 30 Abs. 1 lit. g und Abs. 2 lit. d DSGVO auf § 54 beziehen und die Bezugnahme auf einen Vertreter des Verantwortlichen oder des Auftragsverarbeiters gegenstandslos ist.

(2) Das Verzeichnis gemäß Abs. 1 hat auch Angaben zu enthalten über

1. die Verwendung von Profiling, wenn eine solche Verwendung vorgenommen wird, und
2. die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind.

(3) Jeder Auftragsverarbeiter hat ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten zu führen, das Folgendes enthält:

1. Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Datenschutzbeauftragten,
2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn vom Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation,
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 54 Abs. 1.

Protokollierung

§ 50. (1) Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann.

(2) In automatisierten Verarbeitungssystemen sind alle Verarbeitungsvorgänge in automatisierter Form zu protokollieren. Aus diesen Protokolldaten müssen zumindest der Zweck, die verarbeiteten Daten, das Datum und die Uhrzeit der Verarbeitung, die Identifizierung der Person, die die personenbezogenen Daten verarbeitet hat, sowie die Identität eines allfälligen Empfängers solcher personenbezogenen Daten hervorgehen.

(3) In nicht automatisierten Verarbeitungssystemen sind zumindest Abfragen und Offenlegungen einschließlich Übermittlungen, Veränderungen sowie Löschungen zu protokollieren. Für diese Protokolldaten gilt Abs. 2 zweiter Satz.

(4) Die Protokolle dürfen 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.

(5) Der Verantwortliche und der Auftragsverarbeiter haben der Datenschutzbehörde auf deren Verlangen die Protokolle zur Verfügung zu stellen.

Zusammenarbeit mit der Datenschutzbehörde

§ 51. Der Verantwortliche und der Auftragsverarbeiter sind verpflichtet, über Aufforderung mit der Datenschutzbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten.

Datenschutz-Folgenabschätzung

§ 52. Der Verantwortliche hat zum Schutz der Rechte und berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1, 2, 3, 7 und 11 DSGVO durchzuführen, wobei sich der Nachweis gemäß Art. 35 Abs. 7 lit. d DSGVO auf die Einhaltung der Vorgaben dieses Hauptstücks bezieht.

Vorherige Konsultation der Datenschutzbehörde

§ 53. Der Verantwortliche hat nach Maßgabe des Art. 36 DSGVO vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Datenschutzbehörde zu konsultieren, wobei sich die Verweise in Art. 36 Abs. 1 und Abs. 3 lit. e DSGVO auf § 52 und der Verweis auf die Bestimmungen hinsichtlich der Befugnisse der Datenschutzbehörde in Art. 36 Abs. 2 DSGVO auf § 33 beziehen und die in Art. 36 Abs. 2 DSGVO angeführten Maßnahmen innerhalb von sechs Wochen mit der Möglichkeit einer Verlängerung um einen weiteren Monat zu treffen sind.

Datensicherheitsmaßnahmen

§ 54. (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.

(2) Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle);
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle);
8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung);
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Meldung von Verletzungen an die Datenschutzbehörde

§ 55. (1) Der Verantwortliche hat nach Maßgabe des Art. 33 DSGVO Verletzungen des Schutzes personenbezogener Daten der Datenschutzbehörde zu melden.

(2) Soweit von der Verletzung des Schutzes personenbezogene Daten betroffen sind, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaates der Europäischen Union übermittelt wurden, sind die in Art. 33 Abs. 3 DSGVO genannten Informationen dem Verantwortlichen jenes Mitgliedstaates der Europäischen Union unverzüglich zu übermitteln.

Benachrichtigung der betroffenen Person von Verletzungen

§ 56. (1) Der Verantwortliche hat nach Maßgabe des Art. 34 DSGVO betroffene Personen von Verletzungen des Schutzes ihrer personenbezogenen Daten zu benachrichtigen.

(2) Die Benachrichtigung gemäß Abs. 1 kann unter den in § 43 Abs. 4 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden.

Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

§ 57. (1) Jeder Verantwortliche hat nach Maßgabe des Art. 37 Abs. 5 und 7 DSGVO einen Datenschutzbeauftragten zu benennen. Gerichte sind im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen. § 5 gilt im Hinblick auf die Bestimmungen dieses Hauptstücks sinngemäß.

(2) Für die Stellung des Datenschutzbeauftragten gilt Art. 38 DSGVO.

(3) Dem Datenschutzbeauftragten obliegen die in Art. 39 DSGVO genannten Aufgaben in Bezug auf die Einhaltung der Bestimmungen dieses Hauptstücks.

(4) Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

4. Abschnitt

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

§ 58. (1) Eine Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, durch zuständige Behörden ist nur zulässig, wenn die Bestimmungen dieses Hauptstücks eingehalten werden und

1. die Übermittlung für die in § 36 Abs. 1 genannten Zwecke erforderlich ist,
2. die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in § 36 Abs. 1 genannten Zwecke zuständige Behörde ist, übermittelt werden,
3. in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat der EU übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor genehmigt hat,
4. die Europäische Kommission gemäß § 59 Abs. 1 und 2 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des § 59 Abs. 3 bis 5 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß § 59 Abs. 1 und 2 vorliegt und keine geeigneten Garantien im Sinne des § 59 Abs. 3 bis 5 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß § 59 Abs. 6 und 7 anwendbar sind und
5. sichergestellt ist, dass eine Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation nur aufgrund einer vorherigen Genehmigung der zuständigen Behörde, die die ursprüngliche Übermittlung durchgeführt hat, und unter gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden, zulässig ist.

(2) Eine Übermittlung ohne vorherige Genehmigung gemäß Abs. 1 Z 3 ist nur zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der vorherigen Genehmigung zuständige Behörde ist unverzüglich zu unterrichten.

(3) Ersucht eine zuständige Behörde eines anderen Mitgliedstaates der EU um Genehmigung zur Übermittlung von personenbezogenen Daten, die ursprünglich aus dem Inland übermittelt wurden, an ein Drittland oder eine internationale Organisation gemäß Abs. 1 Z 3, so ist zur Erteilung dieser Genehmigung jene zuständige Behörde zuständig, die die personenbezogenen Daten ursprünglich übermittelt hat, soweit nicht gesetzlich anderes angeordnet ist.

Datenübermittlung an Drittländer oder internationale Organisationen

§ 59. (1) Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist zulässig, wenn die Europäische Kommission gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 im Wege eines Durchführungsaktes beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung. Die Genehmigungspflicht gemäß § 58 Abs. 1 Z 3 bleibt davon unberührt.

(2) Übermittlungen personenbezogener Daten an ein Drittland, an ein Gebiet oder einen oder mehrere spezifischen Sektoren in einem Drittland oder an eine internationale Organisation gemäß den Abs. 3 bis 8 werden durch einen gemäß Art. 36 Abs. 5 der Richtlinie (EU) 2016/680 gefassten Beschluss der Europäischen Kommission zum Widerruf, zur Änderung oder zur Aussetzung eines Beschlusses nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 nicht berührt.

(3) Liegt kein Beschluss nach Abs. 1 vor, so ist die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. der Verantwortliche auf Grund einer Beurteilung der für die Übermittlung personenbezogener Daten maßgeblichen Umstände zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

(4) Bestehen geeignete Garantien gemäß Abs. 3 Z 2 für Kategorien von Übermittlungen, so hat der Verantwortliche die Datenschutzbehörde über diese Kategorien zu unterrichten.

(5) Übermittlungen gemäß Abs. 3 Z 2 sind zu dokumentieren und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der Datenschutzbehörde auf Anforderung zur Verfügung zu stellen.

(6) Wenn weder ein Angemessenheitsbeschluss gemäß Abs. 1 bis 2 vorliegt noch geeignete Garantien gemäß Abs. 3 bis 5 vorhanden sind, so ist nach Maßgabe des Abs. 5 eine Übermittlung

personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer Person,
2. wenn dies zur Wahrung berechtigter Interessen der betroffenen Person gesetzlich vorgesehen ist,
3. zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaates der EU oder eines Drittlandes,
4. im Einzelfall für die in § 36 Abs. 1 genannten Zwecke, oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 36 Abs. 1 genannten Zwecken.

(7) In den Fällen des Abs. 6 Z 4 und 5 ist die Übermittlung nur zulässig, wenn keine das öffentliche Interesse an der Übermittlung überwiegenden Grundrechte und Grundfreiheiten der betroffenen Person der Übermittlung entgegenstehen.

4. Hauptstück
Besondere Strafbestimmungen

Verwaltungsstrafbestimmung

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,
3. sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 verschafft,
4. eine Bildverarbeitung entgegen den Bestimmungen des 3. Abschnittes des 1. Hauptstücks betreibt oder
5. die Einschau gemäß § 22 Abs. 2 verweigert.

(2) Der Versuch ist strafbar.

(3) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 30 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

(6) Das Parlamentarische Datenschutzkomitee ist zuständig für Entscheidungen nach Abs. 1 bis 4, soweit durch die Verwaltungsübertretung personenbezogene Daten aus Verarbeitungen gemäß § 35a Abs. 1 betroffen sind. Dasselbe gilt, soweit personenbezogene Daten aus Verarbeitungen gemäß § 35a Abs. 2 betroffen sind, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

§ 63. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

5. Hauptstück
Schlussbestimmungen

Durchführung und Umsetzung von Rechtsakten der EU

§ 64. (1) Dieses Bundesgesetz dient der Durchführung der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1.

(2) Dieses Bundesgesetz dient weiters der Umsetzung 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.

Sprachliche Gleichbehandlung

§ 65. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Erlassung von Verordnungen

§ 66. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 67. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 68. (1) Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, die Bundesministerin für Justiz sowie der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereichs betraut.

(2) **(Verfassungsbestimmung)** Mit der Vollziehung des 6. Abschnitts des 2. Hauptstücks und des § 62 Abs. 6 ist der Präsident des Nationalrates betraut.

Übergangsbestimmungen

§ 69. (1) Die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes laufende Funktionsperiode des Leiters der Datenschutzbehörde wird bis zu deren Ablauf fortgesetzt. Dies gilt auch für dessen Stellvertreter.

(2) Das von der Datenschutzbehörde geführte Datenverarbeitungsregister ist von der Datenschutzbehörde bis zum 31. Dezember 2019 zu Archivzwecken fortzuführen. Es dürfen keine Eintragungen und inhaltliche Änderungen im Datenverarbeitungsregister vorgenommen werden. Registrierungen im Datenverarbeitungsregister werden gegenstandslos. Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er eine betroffene Person ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Verantwortlichen (Auftraggebers) oder anderer Personen entgegenstehen.

(3) Gemäß den §§ 17 und 18 Abs. 2 DSG 2000 im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Registrierungsverfahren gelten als eingestellt. Im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Verfahren nach den §§ 13, 46 und 47 DSG 2000 sind fortzuführen, sofern die Genehmigung nach diesem Bundesgesetz oder der DSGVO erforderlich ist. Anderenfalls gelten sie als eingestellt.

(4) Zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum Datenschutzgesetz 2000 anhängige Verfahren sind nach den Bestimmungen dieses Bundesgesetzes und der DSGVO fortzuführen, mit der Maßgabe, dass die Zuständigkeit der ordentlichen Gerichte aufrecht bleibt.

(5) Verletzungen des Datenschutzgesetzes 2000, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, sind nach der Rechtslage nach Inkrafttreten dieses Bundesgesetzes zu beurteilen. Ein strafbarer Tatbestand, der vor dem Inkrafttreten dieses Bundesgesetzes

verwirklicht wurde, ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(6) Die Eingaben der betroffenen Personen nach den §§ 24 und 35f sind von den Verwaltungsabgaben des Bundes befreit.

(7) Die entsendenden Stellen haben eine dem § 15 Abs. 1 Z 1 bis 6 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern des Datenschutzrates dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz innerhalb von zwei Wochen ab dem 25. Mai 2018 schriftlich bekannt zu geben. Die konstituierende Sitzung des Datenschutzrates hat innerhalb von sechs Wochen ab dem 25. Mai 2018 zu erfolgen. Bis zur Wahl des neuen Vorsitzenden und der beiden stellvertretenden Vorsitzenden bleiben der bisherige Vorsitzende sowie die beiden bisherigen stellvertretenden Vorsitzenden in ihrer Funktion.

(8) Besondere Bestimmungen über die Verarbeitung von personenbezogenen Daten in anderen Bundes- oder Landesgesetzen bleiben unberührt.

(9) Vor Inkrafttreten dieses Bundesgesetzes nach §§ 13, 46 und 47 DSG 2000 rechtskräftig erteilte Genehmigungen der Datenschutzbehörde bleiben unberührt. Nach dem Datenschutzgesetz 2000 erteilte Zustimmungen bleiben aufrecht, sofern sie den Vorgaben der DSGVO entsprechen.

(10) **(Verfassungsbestimmung)** Das Parlamentarische Datenschutzkomitee hat seine Zuständigkeiten nach diesem Bundesgesetz ab 1. Jänner 2025 wahrzunehmen. Zu diesem Zeitpunkt bei der Datenschutzbehörde anhängige Verfahren betreffend Verarbeitungen gemäß § 35a Abs. 1 sind vom Parlamentarischen Datenschutzkomitee fortzuführen, wobei die Entscheidungsfrist neu zu laufen beginnt. In den beim Bundesverwaltungsgericht, beim Verwaltungsgerichtshof oder beim Verfassungsgerichtshof mit Ablauf des 31. Dezember 2024 anhängigen Verfahren betreffend Verarbeitungen gemäß § 35a Abs. 1 tritt das Parlamentarische Datenschutzkomitee an die Stelle der Datenschutzbehörde.

(11) **(Verfassungsbestimmung)** Abs. 10 gilt auch in Bezug auf Verarbeitungen gemäß § 35a Abs. 2, sofern für die Aufsicht über diese Verarbeitungen durch Landesverfassungsgesetz die Zuständigkeit des Parlamentarischen Datenschutzkomitees vorgesehen wurde.

Inkrafttreten

§ 70. (1) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(2) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

(3) § 48a Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 135/2009 tritt mit 1. Jänner 2010 in Kraft.

(4) Das Inhaltsverzeichnis, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 8 Abs. 1, 2 und 4, § 12 Abs. 1, die Umnummerierung der Absätze in § 13, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a und Abs. 2, die Umnummerierung der Absätze in § 19, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 24 Abs. 4, § 26 Abs. 1 bis 8 und 10, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt, § 51, § 52 Abs. 2 und 4, § 55, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 sowie § 51 Abs. 2 außer Kraft.

(5) § 36 Abs. 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 tritt am 1. Juli 2010 in Kraft.

(6) § 37 Abs. 2, § 38 Abs. 2 und § 61 Abs. 9 in der Fassung des Bundesgesetzes BGBl. I Nr. 57/2013 treten mit 1. Mai 2013 in Kraft.

(7) Das Inhaltverzeichnis, § 5 Abs. 4, § 10 Abs. 2, § 12 Abs. 4, § 13 Abs. 1, 2 Z 2, Abs. 3, 4 und 6, § 16 Abs. 1, § 17 Abs. 1, § 18 Abs. 2, § 19 Abs. 1 Z 6 und Abs. 2, § 20 Abs. 2 und 5 Z 2, § 21 Abs. 1 Z 3, § 22 Abs. 2 bis 4, § 22a Abs. 1, 3 bis 5, § 23 Abs. 2, § 26 Abs. 2, 5 und 7, § 27 Abs. 5 und 7, die Überschrift zu § 30, § 30 Abs. 1, 2, 2a, 4 bis 6a, die Überschrift zu § 31, § 31 Abs. 1, 2, 5, 6 und 8, § 31a, § 32 Abs. 5 bis 7, § 34 Abs. 3 und 4, die Überschrift zu § 35, § 35 Abs. 1, §§ 36 bis 40 samt Überschriften, § 41 Abs. 2 Z 1, § 44 Abs. 6 und 8, § 46 Abs. 2 Z 3 und Abs. 3, § 47 Abs. 3 und 4, § 48a Abs. 2, § 50 Abs. 1 und 2, § 50b Abs. 2, § 50c Abs. 1, § 52 Abs. 2 Z 2 und 3 sowie Abs. 5, § 54 Abs. 2 und § 61 Abs. 8 bis 10 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft. Gleichzeitig treten § 41 Abs. 2 Z 4a und die DSK-Vergütungsverordnung, BGBl. II

Nr. 145/2006, außer Kraft. Die für die Bestellung des Leiters der Datenschutzbehörde und seines Stellvertreters notwendigen organisatorischen und personellen Maßnahmen können bereits vor Inkrafttreten des Bundesgesetzes BGBl. I Nr. 83/2013 getroffen werden.

(8) **(Verfassungsbestimmung)** § 2 Abs. 2 und § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft.

(9) Der Titel, das Inhaltsverzeichnis, das 1. Hauptstück, die Bezeichnung und Überschrift des 2. Hauptstücks, der 1., 2., 3. und 4. Abschnitt, die Überschrift und Bezeichnung des 5. Abschnittes, § 35 Abs. 1, die Bezeichnung und Überschrift des 3. Hauptstücks, der 1., 2. und 3. Abschnitt, die Überschrift und Bezeichnung des 4. Abschnittes, die §§ 58 und 59 samt Überschriften sowie das 4. und 5. Hauptstück in der Fassung des Bundesgesetzes BGBl. I Nr. 120/2017 treten mit 25. Mai 2018 in Kraft. Im Art. 2 treten der 1., 2., 3., 4., 5 und 6. Abschnitt, die Bezeichnung und die Überschrift des 7. Abschnittes, die Überschrift zu § 35, die §§ 36 bis 44 samt Überschriften, der 8., 9., 9a. und 10. Abschnitt, die Bezeichnung und die Überschrift des 11. Abschnittes, die §§ 53 bis 59 samt Überschriften, § 61 Abs. 1 bis 3 und 5 bis 10 sowie die §§ 62 bis 64 samt Überschriften in der Fassung vor der Novelle BGBl. I Nr. 120/2017 mit Ablauf des 24. Mai 2018 außer Kraft.

(10) Die Standard- und Muster-Verordnung 2004 – StMV 2004, BGBl. II Nr. 312/2004, die Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012, BGBl. II Nr. 257/2012, und die Datenschutzangemessenheits-Verordnung – DSAV, BGBl. II Nr. 521/1999, treten mit Ablauf des 24. Mai 2018 außer Kraft.

(11) **(Verfassungsbestimmung)** § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 23/2018 tritt mit 25. Mai 2018 in Kraft.

(12) Das Inhaltsverzeichnis, § 4 Abs. 1, 5 bis 7, § 5 Abs. 3 erster Satz und Abs. 5, § 9 samt Überschrift, § 11 samt Überschrift, § 12 Abs. 3 Z 2 und Abs. 4 Z 3, § 14 Abs. 1, § 15 Abs. 1 Z 5, Abs. 3, Abs. 5 Z 1 und 2, Abs. 6, 7 und 8, § 16 Abs. 3 Z 2 und Abs. 5, § 19 Abs. 2 und 3, § 23 Abs. 1, § 26 Abs. 1, § 28, § 30 Abs. 3 und 5, § 32 Abs. 1 Z 1, § 36 Abs. 1 und 2 Z 7, § 44 Abs. 2, § 49 Abs. 1 und 3, § 56 Abs. 1, § 64 Abs. 2, § 68 sowie § 69 Abs. 5 und 7 in der Fassung des Bundesgesetzes BGBl. I Nr. 24/2018 treten mit 25. Mai 2018 in Kraft. Gleichzeitig tritt § 45 Abs. 7 in der Fassung vor der Novelle BGBl. I Nr. 24/2018 außer Kraft. § 70 Abs. 1 bis 8 in der Fassung des Bundesgesetzes BGBl. I Nr. 24/2018 tritt mit dem auf die Kundmachung folgenden Tag in Kraft. Soweit sich die im Bundesgesetz BGBl. I Nr. 24/2018 getroffenen Anordnungen auf durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, geschaffene Vorschriften beziehen, gehen die Regelungen des Bundesgesetzes BGBl. I Nr. 24/2018 jenen des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, vor.

(13) § 16 Abs. 5 und § 70 Abs. 6, 7, 9, 10 und 12 in der Fassung des Bundesgesetzes BGBl. I Nr. 14/2019 treten mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft; gleichzeitig treten die Einträge zu den §§ 60 und 61 im Inhaltsverzeichnis außer Kraft. Die Einträge zu den §§ 2 und 3 im Inhaltsverzeichnis und § 4 Abs. 7 treten mit 1. Jänner 2020 außer Kraft.

(14) **(Verfassungsbestimmung)** Die §§ 2 und 3 samt Überschriften treten mit Ablauf des 31. Dezember 2019 außer Kraft. § 70 Abs. 8 und 11 in der Fassung des Bundesgesetzes BGBl. I Nr. 14/2019 tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft; gleichzeitig tritt § 61 samt Überschrift außer Kraft.

(15) § 9 Abs. 1 und 1a in der Fassung des Bundesgesetzes BGBl. I Nr. 62/2024 tritt mit 1. Juli 2024 in Kraft. § 8 Abs. 2 Z 2 lit. b und Abs. 3 Z 1, § 14 Abs. 1, § 15 Abs. 1 Z 5, Abs. 3, Abs. 5 Z 1 und 2, Abs. 6, 7 und 8, § 16 Abs. 3 Z 2 und Abs. 5, § 19 Abs. 2 und 3, § 23 Abs. 1 erster und zweiter Satz, § 28, § 36 Abs. 2 Z 10 erster Satz und Z 15, § 37 Abs. 1 Z 2 und 3 und § 68 in der Fassung des Bundesgesetzes BGBl. I Nr. 62/2024 treten mit Ablauf des Tages der Kundmachung in Kraft.

(16) In der Fassung des Bundesgesetzes BGBl. I Nr. 70/2024 treten in Kraft:

1. Das Inhaltsverzeichnis, § 17 Abs. 6 und 8, § 24 Abs. 1 zweiter Satz, die Bezeichnung und die Überschrift des 6. Abschnittes des 2. Hauptstücks, die Überschrift zu § 35b, § 35b Abs. 2, 3 und 5, die Überschrift zu § 35c, § 35c Abs. 1 und 2, § 35d samt Überschrift, die Überschrift zu § 35e, § 35e Abs. 1 und 2, § 35f samt Überschrift, die Überschrift zu § 35g, § 35g Abs. 3, § 35h samt Überschrift, die Bezeichnung und die Überschrift des 7. Abschnittes des 2. Hauptstücks, § 35i und § 35j samt Überschriften, § 62 Abs. 6, § 68 Abs. 1 sowie § 69 Abs. 6 mit 15. Juli 2024;
2. **(Verfassungsbestimmung)** § 35 Abs. 2, § 35a samt Überschrift, § 35b Abs. 1 und 4, § 35c Abs. 3, § 35e Abs. 3, § 35g Abs. 1 und 2, § 68 Abs. 2 sowie § 69 Abs. 10 und 11 mit 15. Juli 2024.

(17) §§ 17 Abs. 8, 22 Abs. 3 und 23 Abs. 2 in der Fassung des Informationsfreiheits-Anpassungsgesetzes, BGBl. I Nr. 50/2025, tritt mit 1. September 2025 in Kraft.