20061

Geltende Gesetze und Verordnungen (SGV. NRW.) mit Stand vom 16.5.2020

Datenschutzgesetz Nordrhein-Westfalen
(DSG NRW)
Vom 17. Mai 2018 (Fn 1)

(Artikel 1 des Gesetzes vom 17. Mai 2018 (GV. NRW. S. 244))

Inhaltsübersicht

Teil 1
Allgemeine Bestimmungen

§ 1
Zweck

(1) Dieses Gesetz trifft die zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) notwendigen ergänzenden Regelungen. Innerhalb der Grenzen der Verordnung (EU) 2016/679 werden spezifische Anforderungen an die Verarbeitung personenbezogener Daten geregelt.

(2) Dieses Gesetz dient ebenfalls der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck 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. L 119 vom 4.5.2016, S. 89).

§ 2
Sicherstellung des Datenschutzes

Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform haben jeweils für ihren Bereich die Ausführung der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

§ 3
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Soweit spezialgesetzliche Regelungen nicht vorgehen, ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe der verarbeitenden Stellen erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(2) Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Sind personenbezogene Daten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgaben erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der betroffenen Person oder Dritter überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(3) Behördliche Unterlagen über die technischen und organisatorischen Maßnahmen gemäß Artikel 32 der Verordnung (EU) 2016/679 unterliegen nicht dem allgemeinen Informationszugang nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen.

§ 4
Begriffsbestimmung

Ergänzend zu Artikel 4 der Verordnung (EU) 2016/679 bezeichnet der Ausdruck „Anonymisieren“ das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

§ 5
Anwendungsbereich

(1) Teil 2 dieses Gesetzes gilt für die Verarbeitung personenbezogener Daten durch die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform (öffentliche Stellen). Unbeschadet der Regelung des Satzes 1 gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, gilt sie als öffentliche Stelle im Sinne des Gesetzes.

(2) Öffentliche Stellen im Sinne dieses Gesetzes sind auch natürliche und juristische Personen des privaten Rechts, soweit sie Befugnisse der Verwaltung übertragen bekommen haben und hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen.

(3) Für den Landtag gilt Teil 2 dieses Gesetzes, soweit er Verwaltungsaufgaben wahrnimmt.

(4) Für den Landesrechnungshof und die Staatlichen Rechnungsprüfungsämter, die Gerichte und die Behörden der Staatsanwaltschaft gilt Teil 2 dieses Gesetzes, soweit sie Verwaltungsaufgaben wahrnehmen.

(5) Teil 2 dieses Gesetzes findet mit Ausnahme des Kapitels 3 Abschnitt 1, des Kapitels 5 und des § 32 keine Anwendung, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über Eigenbetriebe geführt werden,
3. Landesbetriebe oder
4. der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbänden unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen, und die NRW.BANK,

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Soweit Hochschulen im Sinne des § 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG)

Aufgaben nach § 3 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) wahrnehmen findet Satz 1 keine Anwendung.
Soweit dieses Gesetz nach Maßgabe von Satz 1 keine Anwendung findet, gelten die Vorschriften für nicht-öffentliche Stellen mit Ausnahme der §§ 4, 22, 26 bis 28 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung entsprechend.

(6) Soweit besondere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften des Teils 2 dieses Gesetzes vor. Regeln Rechtsvorschriften einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes insoweit Anwendung.

(7) Die Vorschriften der §§ 22-24 und 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie (KunstUrhG) vom 9.1.1907, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16.2.2001 in seiner jeweils geltenden Fassung, bleiben für die nach § 5 unter dieses Gesetz fallenden Stellen unberührt.

(8) Auf Verarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen, sind die Vorschriften der Verordnung (EU) 2016/679 und die Vorschriften des Teils 2 dieses Gesetzes entsprechend anzuwenden, soweit nicht dieser Teil oder andere spezielle Rechtsvorschriften abweichende Regelungen enthalten. Dies gilt nicht für die in den Absätzen 3 und 4 genannten Stellen. Im Fall der entsprechenden Anwendung sind die Vorschriften über den gerichtlichen Rechtsschutz nach § 20 des Bundesdatenschutzgesetzes anzuwenden.

(9) Für Verarbeitungen, die nicht dem Anwendungsbereich von Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 unterfallen, gelten die Artikel 13 und 14 der Verordnung (EU) 2016/679 nicht.

Teil 2
Durchführungsbestimmungen zur Verordnung (EU) 2016/679

Kapitel 1
Grundsätze der Verarbeitung personenbezogener Daten

§ 6
Automatisierte Abrufverfahren und regelmäßige Datenübermittlung

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung gespeicherter personenbezogener Daten an andere öffentliche Stellen ermöglicht, ist zulässig, soweit die Verarbeitung der Daten zur Erfüllung von Zwecken nach Artikel 6 Absatz 1 Buchstabe c oder e der Verordnung (EU) 2016/679 erfolgt und eine Rechtsvorschrift dies zulässt. Die Zulässigkeit des einzelnen Abrufs bestimmt sich nach den Vorschriften der Verordnung (EU) 2016/679 und dieses Gesetzes.

(2) Die obersten Landesbehörden werden ermächtigt, für die Behörden und Einrichtungen ihres Geschäftsbereichs sowie für die der Rechtsaufsicht des Landes unterliegenden sonstigen öffentlichen Stellen die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung zuzulassen. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Die Datenempfänger, die Datenart und der Zweck des Abrufs sind festzulegen. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist frühzeitig zu unterrichten.

(3) Die Absätze 1 und 2 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(4) Für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle gelten Absatz 2 Satz 2 bis 4 sowie Absatz 3 entsprechend.

(5) Für die Zulassung regelmäßiger Datenübermittlungen sind die Absätze 1 bis 4 entsprechend anzuwenden.

§ 7
Erhebung personenbezogener Daten bei dritten Personen und nicht-öffentlichen Stellen

Werden personenbezogene Daten bei einer dritten Person oder einer nicht-öffentlichen Stelle erhoben, so hat die oder der Erhebende diese auf Verlangen über den Erhebungszweck zu informieren, soweit dadurch schutzwürdige Belange der betroffenen Person nicht beeinträchtigt werden. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die sie zur Auskunft verpflichtet, ist die dritte Person beziehungsweise die nicht-öffentliche Stelle auf diese Vorschrift, anderenfalls auf die Freiwilligkeit ihrer Angaben, hinzuweisen.

§ 8
Verantwortung für die Datenübermittlung

(1) Die Verantwortung für die Zulässigkeit einer Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, trägt diese die Verantwortung. Die übermittelnde Stelle hat dann lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn hierzu im Einzelfall Anlass besteht. Die ersuchende Stelle hat in dem Ersuchen die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 3 und § 9 zulassen würden,
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder
3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist
4. und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden.

Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Voraussetzungen des Absatzes 1 oder 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 16 vorliegen.

(4) Bei Übermittlung personenbezogener Daten an nichtöffentliche Stellen ist auf die Voraussetzungen in Absatz 2 und 3 hinzuweisen.

§ 9
Zulässigkeit der Datenverarbeitung im Hinblick auf die Zweckbindung

(1) Personenbezogene Daten dürfen durch öffentliche Stellen auch zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen verarbeitet werden. Dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken, sofern berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen.

(2) Eine Verarbeitung personenbezogener Daten zu anderen Zwecken als zu denjenigen, zu denen die Daten erhoben worden sind, ist zulässig, wenn

1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit erforderlich ist,
2. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
3. sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint,
4. die Überprüfung der Angaben der betroffenen Person aufgrund tatsächlicher Anhaltspunkte für deren Unrichtigkeit erforderlich ist,
5. sie zur Wahrung eines rechtlichen Interesses eines Dritten erforderlich ist und das schützenswerte Geheimhaltungsinteresse der betroffenen Person nicht überwiegt oder
6. sie im öffentlichen Interesse, insbesondere zur Durchsetzung öffentlich-rechtlicher Geldforderungen, liegt oder zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und die betroffene Person in diesen

Fällen der Datenverarbeitung nicht widersprochen hat.

(3) Eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 2 erfolgt nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde.

(4) Ferner ist eine Zweckänderung zulässig, wenn
1. die Einholung der Einwilligung der betroffenen Person nicht möglich ist oder mit unverhältnismäßig hohem Aufwand verbunden wäre, aber offensichtlich ist, dass die Datenverarbeitung in ihrem Interesse liegt und sie in Kenntnis des anderen Zweckes ihre Einwilligung erteilen würde,
2. die Bearbeitung eines von der betroffenen Person gestellten Antrags ohne die Zweckänderung der Daten nicht möglich ist,
3. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die datenverarbeitende Stelle sie veröffentlichen darf, es sei denn, dass das Interesse der betroffenen Person an dem Ausschluss der Speicherung oder einer Veröffentlichung der gespeicherten Daten offensichtlich überwiegt

(5) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der verantwortlichen Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, finden die Absätze 2 und 4 keine Anwendung.

(6) Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

§ 10
Löschung personenbezogener Daten

(1) Sofern öffentliche Stellen verpflichtet sind, einem öffentlichen Archiv Unterlagen zur Übernahme anzubieten, ist eine Löschung personenbezogener Daten erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten und als nicht archivwürdig bewertet worden sind oder die Verpflichtung zur weiteren Aufbewahrung nach § 4 Absatz 5 Satz 1 des Archivgesetzes Nordrhein-Westfalen vom 16. März 2010 (**GV. NRW. S. 188**) in der jeweils geltenden Fassung, entfallen ist.

(2) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Kapitel 2
Rechte der betroffenen Personen

§ 11
Beschränkung der Informationspflicht bei der Erhebung von personenbezogenen Daten nach Artikel 13 und 14 der Verordnung (EU) 2016/679

(1) Bei der Verarbeitung personenbezogener Daten entfällt die Informationspflicht des Verantwortlichen nach Artikel 13 Absatz 3 und Artikel 14 Absätze 1, 2 und 4 der Verordnung (EU) 2016/679, soweit und solange
1. die Information die Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Verstößen, die öffentliche Sicherheit oder den Schutz des Wohles des Bundes oder eines Landes gefährdet,
2. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind oder
3. die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

(2) Bezieht sich die Informationspflicht auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaft, an Polizeidienststellen, an Behörden der Finanzverwaltung, soweit sie personenbezogene

Daten für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten speichern, an Verfassungsschutzbehörden, an den Bundesnachrichtendienst, an den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist die Erteilung der Information nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten von diesen Behörden.

§ 12
Beschränkung des Auskunftsrechts der betroffenen Person nach Artikel 15 der Verordnung (EU) 2016/679

(1) Soweit der Verantwortliche große Mengen von Informationen über die betroffene Person verarbeitet, kann er bei einem Auskunftsersuchen verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Das Auskunftsrecht setzt voraus, dass die betreffende Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglicht.

(2) Die Auskunftserteilung kann abgelehnt werden, soweit und solange
1. dies zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder berufsrechtlichen Verstößen notwendig ist,
2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind.

Die betroffene Person kann keine Auskunft über die Verarbeitung sie betreffender personenbezogener Daten nach Artikel 15 der Verordnung (EU) 2016/679 verlangen, soweit die Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaft, an Polizeidienststellen, an Behörden der Finanzverwaltung, soweit sie personenbezogene Daten für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten speichern, an Verfassungsschutzbehörden, an den Bundesnachrichtendienst, an den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist die Auskunft nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten von diesen Behörden.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Begründung der Zweck der Verweigerung gefährdet würde. Die Ablehnungsgründe sind aktenkundig zu machen.

§ 13
Beschränkung der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach Artikel 34 der Verordnung (EU) 2016/679

Der Verantwortliche kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, soweit und solange
1. die Informationen die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind oder
3. die Information die Sicherheit von IT-Systemen gefährden würde.

§ 14
Beschränkung des Widerspruchsrechts

Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Kapitel 3
Vorschriften für besondere Verarbeitungssituationen

§ 15
Garantien zum Schutz personenbezogener Daten und anderer Grundrechte

Werden besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 verarbeitet, sind vom Verantwortlichen angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorzusehen. 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sind das:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
5. die Anonymisierung und wenn sie nicht möglich ist die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung oder
9. spezifische Verfahrensregelungen, die im Falle einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

Abschnitt 1
Besondere Verarbeitungssituationen im Anwendungsbereich der Verordnung (EU) 2016/679

§ 16
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, soweit

1. sie zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist,
2. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen, von Bußgeldentscheidungen, Maßregeln der Besserung und Sicherung, Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Anordnung von Einziehungsentscheidungen erforderlich ist,
3. sie zum Zwecke der Gesundheitsvorsorge, zur medizinischen Diagnostik, zur Gewährleistung und Überwachung der Gesundheit oder Mitteilung von Gesundheitswarnungen, zur Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren oder zur Verwaltung von Leistungen der Gesundheitsversorgung erforderlich ist, sofern die Verarbeitung dieser Daten durch ärztliches oder sonstiges Personal erfolgt, das einer entsprechenden Geheimhaltungspflicht unterliegt oder
4. sie erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen.

(2) Im Falle des Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 hat die Einwilligung in die Verarbeitung genetischer oder biometrischer Daten oder von Gesundheitsdaten schriftlich zu erfolgen.

§ 17
Datenverarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken

(1) Die Verarbeitung personenbezogener Daten ist aufgrund von Artikel 6 Absatz 1 Satz 1 Buchstabe e) der Verordnung (EU) 2016/679 sowie besonderer Kategorien personenbezogener Daten aufgrund von Artikel 9 Absatz 2 Buchstabe j) der Verordnung (EU) 2016/679, auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und schutzwürdige Belange der betroffenen Person nicht überwiegen.

(2) Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 15 vor. Ergänzend zu den in § 15 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Zuvor sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert. Sie sind zu löschen, sobald der Forschungs- oder Statistikzweck dies erlaubt.

(4) Die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeiteten personenbezogenen Daten einschließlich solcher im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 dürfen nach Maßgabe von Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 nur veröffentlicht werden, wenn

1. die betroffene Person in die Veröffentlichung eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen oder solchen über Ereignisse der Zeitgeschichte erforderlich ist und das öffentliche Interesse die schutzwürdigen Belange der betroffenen Person erheblich überwiegt.

(5) Ansprüche auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679, auf Berichtigung gemäß Artikel 16 der Verordnung (EU) 2016/679, auf Einschränkung der Bearbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679 und auf Widerspruch gemäß Artikel 21 der Verordnung (EU) 2016/679 bestehen nicht, soweit die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung dieser Rechte für die Erfüllung dieser Zwecke notwendig ist.

§ 18
Datenverarbeitung im Beschäftigungskontext

(1) Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht oder die oder der Beschäftigte eingewilligt hat. Eine Übermittlung der Daten von Bewerberinnen und Bewerbern und Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder die betroffene Person eingewilligt hat. Die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen

Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen.

(4) Personenbezogene Daten von Bewerberinnen und Bewerbern für
1. den Polizeivollzugsdienst oder
2. ein Arbeits-, Ausbildungs- oder Praktikantenverhältnis in Polizeibehörden

dürfen zum Zwecke der Überprüfung der Einstellungsvoraussetzungen an Polizei- und Verfassungsschutzbehörden übermittelt werden. Die Daten dürfen in den Vorgangsverwaltungs- und Informationssystemen der Polizei- und der Verfassungsschutzbehörden verarbeitet werden. Eine Einwilligung der Bewerberinnen und Bewerber hierzu ist nicht notwendig.

(5) Die beamtenrechtlichen Vorschriften über die Führung von Personalakten gemäß § 50 des Beamtenstatusgesetzes vom 17. Juni 2008 (BGBl. I S. 1010) in der jeweils geltenden Fassung sowie §§ 83 bis 92 des Landesbeamtengesetzes vom 14. Juni 2016 (GV. NRW. S. 310,
ber. S. 642) in der jeweils geltenden Fassung, sind für alle nicht beamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit nicht die Besonderheiten des Tarif- und Arbeitsrechts hinsichtlich der Aufnahme und Entfernung von bestimmten Vorgängen und Vermerken eine abweichende Behandlung erfordern.

(6) Die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests zum Zwecke der Eingehung eines Beschäftigungsverhältnisses erhobenen Daten ist nur mit schriftlicher Einwilligung der betroffenen Person zulässig. Die Einstellungsbehörde darf vom untersuchenden Arzt in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und der dabei festgestellten Risikofaktoren verlangen.

(7) Personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, dass die betroffene Person in die weitere Speicherung eingewilligt hat oder dass Fristen für die Geltendmachung von Ansprüchen nach dem Allgemeinen Gleichbehandlungsgesetz vom 14. August 2006 (BGBl. I S. 1897) in der jeweils geltenden Fassung abzuwarten sind. Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, wenn diese Daten nicht mehr benötigt werden, es sei denn, dass Rechtsvorschriften der Löschung entgegenstehen.

(8) Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests der Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz der Beschäftigten dient.

(9) Soweit Daten der Beschäftigten im Rahmen der Durchführung von technischen und organisatorischen Maßnahmen nach Artikel 32 der Verordnung (EU) 2016/679 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

(10) Beurteilungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

(11) Leitstellen und Befehlsstellen der in Satz 4 genannten Einrichtungen und Organisationen dürfen zur Bestimmung des geografischen Standorts personenbezogene Daten der von ihnen gesteuerten Einsatzkräfte mittels elektronischer Einrichtungen durch eine Funktion des Digitalfunks für Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Digitalfunk) oder durch andere technische Mittel ohne Einwilligung der betroffenen Person verarbeiten, soweit dies aus dienstlichen Gründen zur Sicherheit oder zur Koordinierung der Einsatzkräfte erforderlich ist. Standortdaten dürfen ausschließlich zu den in Satz 1 festgelegten Zwecken verarbeitet werden. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks der Speicherung nicht mehr erforderlich sind. Die Sätze 1 und 2 gelten für Einsatzkräfte der Berechtigten des § 4 Absatz 1 Nummern 1.1, 1.5, 1.6, 1.7 bis 1.9 der BOS-Funkrichtlinie vom 7. September 2009 (GMBl. 2009, S. 803) in der jeweils geltenden Fassung soweit es sich hierbei um kommunale Behörden oder um Landesbehörden handelt.

(12) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

§ 19
Verarbeitung zu künstlerischen oder literarischen Zwecken

(1) Werden personenbezogene Daten zu künstlerischen oder literarischen Zwecken verarbeitet, stehen den betroffenen Personen nur die in Absatz 2 genannten Rechte zu. Im Übrigen gelten für Verarbeitungen im Sinne des Satzes 1 Kapitel I, Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und 32, Kapitel VIII, X und XI der Verordnung (EU) 2016/679. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird.

(2) Führt die künstlerische oder literarische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen, zu Verpflichtungserklärungen, gerichtlichen Entscheidungen oder Widerrufen, sind diese zu den gespeicherten Daten zu nehmen, dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

§ 20
Videoüberwachung

(1) Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Bereichen mittels optisch-elektronischer Einrichtungen (Videoüberwachung) durch öffentliche Stellen ist zulässig, wenn dies

1. zur Wahrnehmung des Hausrechts,
2. zum Schutz des Lebens, der Gesundheit, des Eigentums oder Besitzes oder
3. zur Kontrolle von Zugangsberechtigungen

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Der Umstand der Videoüberwachung, die Angaben nach Artikel 13 Absatz 1 Buchstabe a bis c der Verordnung (EU) 2016/679 sowie die Möglichkeit, bei der oder dem Verantwortlichen die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 zu erhalten, sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten zu einem anderen Zweck ist nur zulässig, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen gegenüber betroffenen Personen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.

(4) Die nach Absatz 1 erhobenen Daten sind unverzüglich zu löschen. Dies gilt nicht, sofern die Daten zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen gegenüber der betroffenen Person erforderlich sind.

Abschnitt 2
Besondere Verarbeitungssituationen außerhalb des Anwendungsbereiches der Verordnung (EU) 2016/679

§ 21
Anwendbarkeit der Verordnung (EU) 2016/679

Auf die Regelungen dieses Abschnitts findet abweichend von der Regelung in § 5 Absatz 8 die Verordnung (EU) 2016/679 grundsätzlich keine entsprechende Anwendung, soweit nicht die Vorschriften dieses Abschnitts die Anwendung einzelner Vorschriften vorsehen.

§ 22
Öffentliche Auszeichnungen und Ehrungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen dürfen die zuständigen Stellen die dazu erforderlichen Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Kenntnis der betroffenen Person verarbeiten. Eine Verarbeitung dieser Daten für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig.

(2) Auf Anforderung der in Absatz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung oder Ehrung erforderlichen Daten übermitteln.

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn der datenverarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat.

(4) In Verfahren der Entscheidung über öffentliche Auszeichnungen und Ehrungen finden nur Artikel 5 bis 7, Kapitel IV mit Ausnahme der Artikel 33 und 34 sowie Kapitel VI der Verordnung (EU) 2016/679 entsprechende Anwendung.

§ 23
Begnadigungsverfahren

(1) In Begnadigungsverfahren ist die Verarbeitung personenbezogener Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, soweit sie zur Ausübung des Gnadenrechts durch die zuständigen Stellen erforderlich ist. Die Datenverarbeitung unterliegt nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit.

(2) In Begnadigungsverfahren finden nur Artikel 5 bis 7 sowie Kapitel IV mit Ausnahme der Artikel 33 und 34 der Verordnung (EU) 2016/679 entsprechende Anwendung.

Kapitel 4
Pflichten des Verantwortlichen

§ 24
Datenschutz-Folgenabschätzung

(1) Eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 1 Satz 1 der Verordnung (EU) 2016/679 soll nicht durchgeführt werden, soweit diese für eine Verarbeitung, die im Wesentlichen unverändert übernommen wird, bereits von der fachlich zuständigen obersten Landesbehörde oder von einer durch diese ermächtigten öffentlichen Stelle durchgeführt wurde.

(2) Die obersten Landesbehörden können den öffentlichen Stellen ihres Geschäftsbereichs die Ergebnisse der von ihnen oder durch von ihnen ermächtigten Behörden durchgeführten Datenschutz-Folgenabschätzungen zur Verfügung stellen, soweit die Information nicht die Sicherheit von IT-Systemen gefährden würde.

(3) Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Artikel 35 Absatz 1 der Verordnung (EU) 2016/679 bei diesem Verfahren vorliegen, die Folgenabschätzung nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 durchführen. Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.

Kapitel 5
Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

§ 25
Errichtung und Rechtsstellung

(1) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist Aufsichtsbehörde im Sinne des Artikels 51 der Verordnung (EU) 2016/679. Der Landtag wählt auf Vorschlag der Landesregierung die Leiterin oder den Leiter der Aufsichtsbehörde für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die Leiterin oder der Leiter der Aufsichtsbehörde für den Datenschutz ist zugleich die oder der Landesbeauftragte für Informationsfreiheit. Sie oder er muss die Befähigung zum Richteramt oder zu der Laufbahngruppe 2, zweites Einstiegsamt haben und die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde und Erfahrung gemäß Artikel 53 Absatz 2 der Verordnung (EU) 2016/679 besitzen. Die Amts- und Funktionsbezeichnung lautet „Die Landesbeauftragte für Datenschutz und Informationsfreiheit“ oder „Der Landesbeauftragte für Datenschutz und Informationsfreiheit“.

(2) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist eine von der Landesregierung unabhängige Landesbehörde. Die Behörde hat ihren Sitz in Düsseldorf. Sie oder er ist oberste Dienstbehörde und trifft Entscheidungen nach § 37 des Beamtenstatusgesetzes vom 17. Juni 2008 (BGBl. I S. 1010) in der

jeweils geltenden Fassung für sich und ihre oder seine Bediensteten in eigener Verantwortung. Die Bediensteten unterstehen nur ihren oder seinen Weisungen.

(3) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit wird jeweils für die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. Die einmalige Wiederwahl ist zulässig. Nach Ende der Amtszeit bleibt sie oder er bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers im Amt. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit bestellt eine Mitarbeiterin zur Stellvertreterin oder einen Mitarbeiter zum Stellvertreter. Diese oder dieser führt die Geschäfte im Verhinderungsfall.

(4) Für die beamtenrechtlichen Angelegenheiten der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit in Person ist das für Inneres zuständige Ministerium mit der Maßgabe zuständig, dass die Wahrnehmung der Zuständigkeit die Unabhängigkeit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nicht beeinträchtigt.

(5) Das Amtsverhältnis beginnt mit Aushändigung der Ernennungsurkunde. Das Amtsverhältnis endet neben den in Artikel 53 Absatz 3 der Verordnung (EU) 2016/679 genannten Gründe mit dem Rücktritt der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit. Über eine Amtsenthebung wegen schwerer Verfehlung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit in Person entscheiden die Richterdienstgerichte. Auf das Verfahren vor den Richterdienstgerichten sind die Vorschriften des Landesrichter- und Staatsanwältegesetzes vom 8. Dezember 2015 (**GV. NRW. S. 812**) in der jeweils geltenden Fassung anzuwenden. Die nach diesen Vorschriften zustehenden Befugnisse der verfahrenseinleitenden Stelle übt die Präsidentin oder der Präsident des Landtags aus. Die nicht ständigen Beisitzerinnen und Beisitzer des Richterdienstgerichts müssen Mitglieder der Verwaltungsgerichtsbarkeit sein.

(6) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit wird im Einzelplan des Landtags in einem eigenen Kapitel ausgewiesen. § 28 Absatz 3 und § 29 Absatz 3 der Landeshaushaltsordnung in der Fassung der Bekanntmachung vom 26. April 1999 (**GV. NRW. S. 158**) in der jeweils geltenden Fassung gelten entsprechend. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit unterliegt der Rechnungsprüfung durch den Landesrechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(7) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist für alle beamten- und disziplinarrechtlichen Entscheidungen sowie für alle arbeitsrechtlichen Entscheidungen ihren oder seinen Beschäftigten gegenüber zuständig. Ihre Einbeziehung in den Personalaustausch in der Landesverwaltung wird gewährleistet. Näheres zur Personalgewinnung und zur Personalverwaltung kann die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit mit dem für Inneres zuständigen Ministerium vereinbaren.

(8) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kann sich jederzeit an den Landtag wenden.

§ 26
Zuständigkeit

Als Aufsichtsbehörde überwacht die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit die Einhaltung der datenschutzrechtlichen Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679, dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz bei den öffentlichen Stellen. Für nicht-öffentliche Stellen und solche im Sinne von § 5 Absatz 5 ist sie oder er Aufsichtsbehörde nach § 40 des Bundesdatenschutzgesetzes.

§ 27
Aufgaben

(1) Neben den sonstigen in Artikel 57 der Verordnung (EU) 2016/679 genannten Aufgaben berät und informiert die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit die öffentlichen Stellen in Belangen des Datenschutzes.

(2) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit bei der Erfüllung ihrer oder seiner Aufgaben und Befugnisse nach

Maßgabe von Artikel 57 und 58 der Verordnung (EU) 2016/679 zu unterstützen und Amtshilfe zu leisten. Der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist jederzeit Zutritt zu allen Diensträumen und Zugriff auf elektronische Dienste zu gewähren. Gesetzliche Geheimhaltungsvorschriften können einem Auskunfts- oder Einsichtsverlangen nicht entgegengehalten werden.

(3) Abweichend von Absatz 2 bestehen die Untersuchungsbefugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 gegenüber den in § 203 Absatz 1 und 3 sowie Absatz 4 Satz 1 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

(4) Sofern die Bereitstellung der geforderten Informationen die Aufgabenerfüllung des Verantwortlichen wesentlich gefährden würde, ist die Gefährdung der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit schriftlich anzuzeigen und zu begründen. Stellt die jeweils zuständige oberste Landesbehörde im Einzelfall fest, dass die Sicherheit des Bundes oder eines Landes dies gebietet, können die Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nur von dieser oder diesem persönlich ausgeübt werden. In diesem Fall müssen personenbezogene Daten einer betroffenen Person, der von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihr oder ihm gegenüber nicht offenbart werden.

(5) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist frühzeitig über Planungen zur Entwicklung, zum Aufbau oder zur wesentlichen Veränderung automatisierter Datenverarbeitungs- und Informationssysteme zu unterrichten, sofern in dem jeweiligen System personenbezogene Daten verarbeitet werden sollen. Entsprechendes gilt für Entwürfe für Rechts- oder Verwaltungsvorschriften des Landes, wenn sie eine Verarbeitung personenbezogener Daten vorsehen.

§ 28
Befugnisse

(1) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist befugt, personenbezogene Daten, die ihr oder ihm durch Beschwerden, Anfragen, Hinweise und Beratungswünsche bekannt werden, zu verarbeiten, soweit dies zur Erfüllung ihrer oder seiner Aufgaben erforderlich ist. Sie oder er darf im Rahmen von Kontrollmaßnahmen personenbezogene Daten auch ohne Kenntnis der betroffenen Person erheben. Von einer Benachrichtigung der betroffenen Person kann nach pflichtgemäßem Ermessen abgesehen werden.

(2) Kommt die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit zu dem Ergebnis, dass Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, kann sie oder er diese

1. bei der Landesverwaltung der zuständigen obersten Landesbehörde, beim Landesrechnungshof der Präsidentin oder dem Präsidenten,
2. bei der Kommunalverwaltung der jeweils verantwortlichen Gemeinde oder dem verantwortlichen Gemeindeverband,
3. bei den wissenschaftlichen Hochschulen und Fachhochschulen der Hochschulpräsidentin oder dem Hochschulpräsidenten oder der Rektorin oder dem Rektor, bei öffentlichen Schulen der Leitung der Schule oder
4. bei den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts dem Vorstand oder dem sonst vertretungsberechtigten Organ

beanstanden und kann vor Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstabe b bis g, i und j der Verordnung (EU) 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist geben. In den Fällen von Satz 1 Nummer 2 bis 4 unterrichtet die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit gleichzeitig auch die zuständige Aufsichtsbehörde. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht.

(3) Die Stellungnahme nach Absatz 2 Satz 1 soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die in Absatz 2 Nummer 2 bis 4 genannten Stellen leiten der zuständigen Rechts- oder Fachaufsichtsbehörde eine Abschrift ihrer Stellungnahme an die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit unverzüglich zu.

§ 29
Beschwerderecht nach Artikel 77 der Verordnung (EU) 2016/679

Jeder kann sich gemäß Artikel 77 der Verordnung (EU) 2016/679 an die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit mit dem Vorbringen wenden, bei der Verarbeitung personenbezogener Daten in seinen Rechten verletzt worden zu sein. Durch die Anrufung der oder des Landesbeauftragten dürfen der betroffenen Person keine Nachteile entstehen. Bei der Ausübung des Beschwerderechts durch Beschäftigte öffentlicher Stellen muss der Dienstweg nicht eingehalten werden.

§ 30
Tätigkeitsbericht, Gutachtertätigkeit

(1) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kann ihren oder seinen nach Maßgabe von Artikel 59 der Verordnung (EU) 2016/679 zu erstellenden Jahresbericht in jedem zweiten Kalenderjahr um eine Darstellung ihrer oder seiner Tätigkeiten auf dem Gebiet der Informationsfreiheit ergänzen. Der Bericht zur Informationsfreiheit ist inhaltlich klar von dem nach Artikel 59 der Verordnung (EU) 2016/679 zu erstellenden Tätigkeitsbericht zu trennen. Eine gemeinsame Veröffentlichung ist zulässig. Der Bericht ist dem Landtag sowie der Landesregierung vorzulegen. Die Landesregierung nimmt hierzu gegenüber dem Landtag schriftlich Stellung.

(2) Der Landtag kann die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit mit der Erstattung von Gutachten in Datenschutzfragen betrauen.

Kapitel 6
Die oder der behördliche Datenschutzbeauftragte

§ 31
Verschwiegenheitspflicht, Zeugnisverweigerungsrecht und Abberufung

(1) Bei Bedarf kann eine Stelle auch mehrere behördliche Datenschutzbeauftragte sowie mehrere Vertreterinnen und Vertreter benennen.

(2) Betroffene Personen können die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der behördliche Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit ist.

(3) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

(4) Die Abberufung der oder des behördlichen Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig. Dies gilt nicht, wenn die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

Kapitel 7
Straf- und Bußgeldvorschriften

§ 32
Geldbußen

Geldbußen nach Artikel 83 der Verordnung (EU) 2016/679 dürfen nur gegen öffentliche Stellen im Sinne des § 5 Absatz 5 Nummer 1 bis 4 verhängt werden.

§ 33
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften der Verordnung (EU) 2016/679, dieses Gesetzes oder einer anderen Rechtsvorschrift des Landes Nordrhein-Westfalen geschützte personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verwendet, verändert, übermittelt, weitergibt, zum Abruf bereit hält, den Personenbezug herstellt oder löscht oder
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung oder Weitergabe an sich oder andere veranlasst.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne von § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602) in der jeweils geltenden Fassung ist die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit.

(4) Gegen öffentliche Stellen im Sinne von § 5 Absatz 1 werden Geldbußen nach Absatz 2 oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten nicht verhängt.

§ 34
Straftaten

(1) Wer in Ausübung seiner Tätigkeit für eine öffentliche Stelle einen der in § 33 Absatz 1 genannten Verstöße gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter sowie die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit.

(3) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

Teil 3
Umsetzung der Richtlinie (EU) 2016/680

Kapitel 1
Allgemeine Bestimmungen

§ 35
Anwendungsbereich

(1) Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch

1. die Behörden der Polizei,
2. die Gerichte in Strafsachen und die Staatsanwaltschaften,
3. die Strafvollstreckungs- und Justizvollzugsbehörden,
4. die Behörden des Maßregelvollzugs und
5. die Behörden der Finanzverwaltung

im Rahmen ihrer Aufgabenwahrnehmung zur Verhütung, Ermittlung, Aufdeckung, Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten und der Strafvollstreckung. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor sowie die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.

(2) Für Ordnungsbehörden gelten die Vorschriften dieses Teils, soweit sie Ordnungswidrigkeiten verfolgen, ahnden sowie Sanktionen vollstrecken.

(3) Soweit besondere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

§ 36
Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (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 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, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, 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, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen,
5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die 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 Daten keiner betroffenen Person zugewiesen werden,
6. „Anonymisierung“ das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten, Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,
7. „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,
8. „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 oder Ordnung, zuständig ist, oder
   b) eine andere Stelle oder Einrichtung, der durch das nationale Recht 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 oder Ordnung, übertragen wurde,
9. „Verantwortlicher“ die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet,
10. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet,
11. „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 nach dem Unionsrecht oder anderen Rechtsvorschriften 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,

12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden,
13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden,
14. „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, insbesondere Gesichtsbilder oder daktyloskopische Daten,
15. „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,
16. „Aufsichtsbehörde“ ist die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit gemäß § 60 dieses Gesetzes,
17. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde,
18. „besondere Kategorien personenbezogener Daten“
  a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen,
  b) genetische Daten,
  c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
  d) Gesundheitsdaten und
  e) Daten zum Sexualleben oder zur sexuellen Orientierung,
19. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist,
20. „öffentliche Stellen“ sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

Kapitel 2
Grundsätze

§ 37
Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen
1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung darf nicht außer Verhältnis zu diesem Zweck stehen,
4. 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. 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, und
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

§ 38
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, und bei einer beabsichtigten Übermittlung über die Empfänger der Daten aufzuklären. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 39
Verarbeitung zu einem anderen Zweck als dem Erhebungszweck

Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben worden sind, ist zulässig, wenn es sich bei dem anderen Zweck um einen solchen in § 35 genannten Zweck handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 35 nicht genannten Zweck, ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 40
Verarbeitung zu wissenschaftlichen oder statistischen Zwecken

Personenbezogene Daten dürfen im Rahmen der in § 35 genannten Zwecke in wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen sind. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 41
Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es auch nach Beendigung ihrer Tätigkeit untersagt, solche Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren.

§ 42
Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,
2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,
3. verurteilte Straftäter,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 43
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 44
Verfahren bei Übermittlungen

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann durch eine entsprechende Markierung der Daten erfüllt werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union 2012/C 326/01 (ABl. C 326 vom 26.10.2012, S. 1) errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 45
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere solche des § 15 sein.

§ 46
Automatisierte Einzelentscheidungen

(1) Entscheidungen, die für die betroffene Person mit einer nachteiligen Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatische Verarbeitung, einschließlich Profiling, gestützt werden, es sei denn eine Rechtsvorschrift lässt dies ausdrücklich zu.

(2) Unbeschadet der allgemeinen Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten dürfen diese bei Entscheidungen nach Absatz 1 nur verarbeitet werden, wenn geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Kapitel 3
Rechte der betroffenen Personen

§ 47
Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,
2. die im Hinblick auf die Verarbeitung der personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
3. die Kontaktdaten des Verantwortlichen und die Kontaktdaten des behördlichen Datenschutzbeauftragten,
4. das Recht nach § 60, die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit anzurufen, und
5. die Erreichbarkeit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit.

§ 48
Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 47 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung soweit und solange aufschieben, einschränken oder unterlassen, wie es

1. die Erfüllung der in § 35 genannten Aufgaben,
2. die öffentliche Sicherheit oder Ordnung,
3. Rechtsgüter Dritter,
4. die Vermeidung von Nachteilen für das Wohl des Bundes oder des Landes sowie
5. die Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

erfordern, wenn das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder, soweit die Sicherheit des Bundes berührt ist, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall des Absatzes 2 gilt § 49 Absatz 8 entsprechend.

§ 49
Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,
7. das Recht nach § 60, die Landesbeauftrage oder den Landesbeauftragten für Datenschutz und Informationsfreiheit anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit.

(2) Die betroffene Person kann keine Auskunft über die Verarbeitung sie betreffender personenbezogener Daten nach Absatz 1 verlangen, soweit die Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Soweit der Verantwortliche große Mengen von Informationen über die betroffene Person verarbeitet, kann er bei einem Auskunftsersuchen verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 48 Absatz 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 ganz oder teilweise einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder, soweit die Sicherheit des Bundes berührt ist, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Information eine Gefährdung im Sinne des § 48 Absatz 2 mit sich bringt. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährdet.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit ausüben. Der Verantwortliche hat die betroffene Person darüber zu unterrichten, dass sie gemäß § 60 die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit anrufen, ihr Auskunftsrecht über sie oder ihn ausüben oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit hat die betroffene Person ebenfalls über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 50
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung

der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder die Daten zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

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

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen dritten Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 35 dienen, weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Information eine Gefährdung im Sinne des § 48 Absatz 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährdet.

(7) § 49 Absatz 7 und 8 finden entsprechende Anwendung.

§ 51
Verfahren

(1) Der Verantwortliche hat mit den betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unverzüglich, unbeschadet des § 49 Absatz 6 und des § 50 Absatz 6, schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 47, die Benachrichtigungen nach § 50 und den Vorschriften über die Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten und die Bearbeitung von Anträgen nach den §§ 49 und 50 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 49 und 50 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 49 oder 50 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung

ihrer Identität erforderlich sind.

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 52
Verarbeitung personenbezogener Daten im Auftrag

(1) Bei der Verarbeitung personenbezogener Daten im Auftrag finden Artikel 28 Absatz 1 bis 4, 9 und 10, sowie Artikel 29 der Verordnung (EU) 2016/679 entsprechende Anwendung. Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Artikel 28 Absatz 1 bis 4, 9 und 10, sowie Artikel 29 der Verordnung (EU) 2016/679 sind auch dann entsprechend anzuwenden, wenn die Prüfung oder Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen durch andere Personen oder Stellen im Auftrag vorgenommen wird. Diese Personen müssen die notwendige fachliche Qualifikation und Zuverlässigkeit aufweisen. Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidlich ist. Dies gilt auch für die Kenntnisnahme von Daten, die Berufs- oder besonderen Amtsgeheimnissen unterliegen. Der Auftragnehmer hat dem Auftraggeber zuzuordnende personenbezogene Daten unverzüglich nach Erledigung des Auftrags zu löschen. Die Dokumentation der Maßnahme ist zum Zweck der Datenschutzkontrolle drei Jahre aufzubewahren.

§ 53
Verzeichnis von Verarbeitungstätigkeiten

Der Verantwortliche und der Auftragsverarbeiter sowie gegebenenfalls deren Vertreter haben ein Verzeichnis ihrer Verarbeitungstätigkeiten zu führen. Artikel 30 Absatz 1 bis 4 der Verordnung (EU) 2016/679 gilt entsprechend mit der Maßgabe, dass in die Verzeichnisse nach Artikel 30 Absatz 1 der Verordnung (EU) 2016/679 ergänzend Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind, sowie gegebenenfalls die Verwendung von Profiling aufzunehmen sind.

§ 54
Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) § 50 Absatz 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist dies dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschungsfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 55
Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,

5. Kombination und
6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten, die Landesbeauftragte für Datenschutz und Informationsfreiheit oder den Landesbeauftragten für Datenschutz und Informationsfreiheit und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

§ 56
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge, hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den berechtigten Interessen der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest die in Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 genannten Anforderungen zu beachten.

(5) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

§ 57
Konsultation der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu konsultieren, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 56 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hat, wenn der Verantwortliche oder Auftragsverarbeiter keine Abhilfemaßnahmen zur Eindämmung des Risikos trifft, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 56 durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstößt, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren. Die Frist nach Satz 1 beginnt erst, sobald die in Absatz 2 Satz 1 benannten, vorzulegenden Pflichtunterlagen vollständig eingereicht wurden. Auch wird die Frist solange gehemmt, bis der Verantwortliche alle Unterlagen, die nach Absatz 2 Satz 2 angefordert wurden, eingereicht hat.

(4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist, beginnen. In diesem Fall sind die Empfehlungen der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit im Nachhinein zu berücksichtigen. Art und Weise der Verarbeitung sind gegebenenfalls anzupassen.

(5) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist bei der Ausarbeitung eines Vorschlags einer zu erlassenden Gesetzgebungsmaßnahme oder von auf solchen Gesetzgebungsmaßnahmen beruhenden Regelungsmaßnahmen, die die Verarbeitung im Anwendungsbereich des § 35 betreffen, zu konsultieren.

§ 58
Anforderungen an die Sicherheit der Verarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass
1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer Verarbeitung personenbezogener Daten haben der Verantwortliche und der Auftragsverarbeiter auf Grundlage einer Risikobewertung Maßnahmen zu ergreifen, die geeignet sind zu gewährleisten, dass
1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität) und
5. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(4) Zur Umsetzung von Absatz 2 sind insbesondere
1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, 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. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle),
9. zu verhindern, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle),
11. zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
12. zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),
13. zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
14.zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität) und
15. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 59
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Das Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde nach Artikel 33 der Verordnung (EU) 2016/679 findet entsprechende Anwendung. Soweit die Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betrifft, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaats übermittelt wurden, sind die in Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 genannten Informationen dem Verantwortlichen des Mitgliedstaats unverzüglich zu übermitteln. Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen die meldepflichtige Person oder einen ihrer in § 54 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung verwendet werden.

Kapitel 5
Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

§ 60
Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

(1) Die Aufsicht über die Einhaltung und Überwachung der Vorschriften dieses Teils sowie anderer Vorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten zu Zwecken des § 35 obliegt der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Artikel 51 bis 55 der Verordnung (EU) 2016/679 und die zu ihrer Durchführung erlassenen Vorschriften dieses Gesetzes finden entsprechende Anwendung.

(2) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit nimmt die Aufgaben nach Artikel 57 Absatz 1 Buchstaben a bis i, l und t, Absatz 2 bis 4 der Verordnung (EU) 2016/679 entsprechend wahr. Übt sie oder er für die betroffene Person deren Rechte aus, hat sie oder er die Rechtmäßigkeit der Verarbeitung zu überprüfen. Die betroffene Person ist innerhalb einer angemessenen Frist über das Ergebnis dieser Überprüfung oder über die Gründe zu unterrichten, aus denen die Überprüfung nicht vorgenommen wurde.

(3) Im Übrigen stehen der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Befugnisse nach Artikel 58 Absatz 1 Buchstabe e, Absatz 2 Buchstabe a, d und f, Absatz 3 Buchstabe a und b, Absatz 4 und 5 der Verordnung (EU) 2016/679 entsprechend zu.

(4) Artikel 59 der Verordnung (EU) 2016/679 gilt entsprechend mit der Maßgabe, dass der Jahresbericht über die Tätigkeit der Aufsichtsbehörde auch eine Liste der Arten der verhängten Sanktionen enthalten kann.

§ 61
Recht auf Beschwerde bei einer Aufsichtsbehörde

Artikel 77 der Verordnung (EU) 2016/679 gilt entsprechend. Jeder kann sich gemäß Artikel 77 der Verordnung (EU) 2016/679 an die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit mit dem Vorbringen wenden, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Durch die Anrufung der oder des Landesbeauftragten dürfen der betroffenen Person keine Nachteile entstehen. Bei der Ausübung des Beschwerderechts durch Beschäftigte öffentlicher Stellen muss der Dienstweg nicht eingehalten werden. Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer anderen Aufsichtsbehörde fällt, unverzüglich an die zuständige Aufsichtsbehörde weiterzuleiten. In diesem Fall hat sie oder er die betroffene Person über die Weiterleitung zu unterrichten und ihr auf ihr Ersuchen weitere Unterstützung zu leisten.

Kapitel 6
Datenübermittlungen an Drittstaaten und an internationale Organisationen

§ 62
Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 35 genannten Zwecke zuständig ist und
2. die Europäische Kommission gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nummer 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige

Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 63
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 62 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 59 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Absatz 1 Nummer 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Landesbeauftragte für Datenschutz und Informationsfreiheit oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 64
Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 62 Absatz 1 Nummer 2 kein Beschluss nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 63 Absatz 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 62 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 35 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 35 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 63 Absatz 2 entsprechend.

§ 65
Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 63 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 62 Absatz 1 Nummer 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 62 Absatz 1 Nummer 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 63 Absatz 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Regelungen in bi- oder multilateralen internationalen Übereinkünften mit Dritten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

Kapitel 7
Ergänzende Vorschriften

§ 66
Vertrauliche Meldung von Datenschutzverstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

§ 67
Ergänzende Anwendung der Verordnung (EU) 2016/679

Die Vorschriften der Verordnung (EU) 2016/679 über

1. den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung nach Artikel 25 Absatz 1 und 2,
2. gemeinsam für die Verarbeitung Verantwortliche gemäß Artikel 26,
3. die Verarbeitungen unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters nach Artikel 29,
4. die Zusammenarbeit mit der Aufsichtsbehörde nach Artikel 31,
5. die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gemäß Artikel 34,
6. die Benennung, Stellung und Aufgaben des behördlichen Datenschutzbeauftragten nach Artikel 37 bis Artikel 39,
7. die gegenseitige Amtshilfe nach Artikel 61 und
8. das Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde nach Artikel 78 Absatz 1 bis 3

sowie die zu ihrer Durchführung erlassenen Vorschriften des Teils 2 dieses Gesetzes sind auf Datenverarbeitungen im Sinne von § 1 Absatz 2 dieses Gesetzes entsprechend anzuwenden.

§ 68
Schadensersatz

(1) Wird der betroffenen Person durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung ihrer personenbezogenen Daten ein Schaden zugefügt, ist der Träger der verantwortlichen Stelle ihr zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(4) Auf eine schuldhafte Mitverursachung des Schadens durch die betroffene Person sind die §§ 254 und 839 Absatz 3 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden. Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

(5) Weitergehende Schadensersatzansprüche bleiben unberührt.

§ 69
Straf- und Bußgeldvorschriften

Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 35 finden die §§ 33 und 34 entsprechende Anwendung.

Teil 4
Übergangsvorschrift, Einschränkung von Grundrechten, Inkrafttreten, Außerkrafttreten

§ 70
Übergangsvorschrift

(1) Mit Inkrafttreten dieses Gesetzes wird das bestehende Amtsverhältnis der Landesbeauftragten für Datenschutz und Informationsfreiheit in ein solches nach diesem Gesetz überführt. Ihre statusrechtliche Stellung bleibt unberührt.

(2) Abweichend von § 53 gelten bis zum 6. Mai 2023 für vor dem 6. Mai 2016 bereits eingeführte Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten im Anwendungsbereich von Teil 3 dieses Gesetzes die Vorschriften über Verfahrensverzeichnisse und Dokumentationen aus den §§ 8 und 10 Absatz 3 des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 (**GV. NRW. S. 542**) in der bis zum 24. Mai 2018 geltenden Fassung.

(3) Abweichend von § 55 gelten bis zum 6. Mai 2023 für vor dem 6. Mai 2016 bereits eingeführte Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten im Anwendungsbereich von Teil 3 dieses Gesetzes die Vorschriften über Protokollierungen nach § 10 Absatz 2 des Datenschutzgesetzes Nordrhein-Westfalen in der bis zum 24. Mai 2018 geltenden Fassung.

§ 71
Einschränkung von Grundrechten

Durch dieses Gesetz werden das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Schutz personenbezogener Daten nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes in Verbindung mit Artikel 4 Absatz 1 und Artikel 4 Absatz 2 Satz 1 der Verfassung für das Land Nordrhein-Westfalen eingeschränkt.

§ 72
Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft. Gleichzeitig tritt das Datenschutzgesetz Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 außer Kraft.

Die Landesregierung
Nordrhein-Westfalen

Der Ministerpräsident

Der Minister der Finanzen

Der Minister des Innern zugleich für den Minister der Justiz

Der Minister für Wirtschaft, Innovation, Digitalisierung und Energie

Der Minister für Arbeit, Gesundheit und Soziales

Die Ministerin für Schule und Bildung
zugleich für den Minister für Kinder, Familie, Flüchtlinge und Integration

Die Ministerin für Heimat, Kommunales, Bau und Gleichstellung

Der Minister für Verkehr,
zugleich für das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz,
insofern mit der Wahrnehmung der Geschäfte beauftragt

Die Ministerin für Kultur und Wissenschaft

Der Minister für Bundes- und Europaangelegenheiten sowie Internationales

Hinweis:
Vollzitat, starre Verweisung: „Datenschutzgesetz Nordrhein-Westfalen vom 17. Mai 2018 (GV. NRW. S. 244, ber. S. 278 und S. 404)“

Fußnoten :

Fn 1 In Kraft getreten am 25. Mai 2018 (GV. NRW. S. 244, ber. S. 278 und S. 404).