LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/1981**

20.02.2018

Gesetzentwurf

der Landesregierung

Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU)

A Problem

Am 25. Mai 2016 ist die 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. Mai 2016, S. 1 ff.) in Kraft getreten. Gemäß Artikel 99 Absatz 2 der Verordnung (EU) 2016/679 gilt sie ab dem 25. Mai 2018. Die Verordnung (EU) 2016/679 weist zum einen Öffnungsklauseln für den nationalen Gesetzgeber, zum anderen konkrete Regelungsaufträge auf. Daraus ergibt sich ein Anpassungsbedarf im allgemeinen Datenschutzrecht des Landes.

Daneben ist die 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 Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89 ff.) in Kraft getreten und bis zum 6. Mai 2018 umzusetzen. Soweit die Mitgliedstaaten nach Artikel 63 der Richtlinie (EU) 2016/680 verpflichtet sind, Rechts- und Verwaltungsvorschriften zu erlassen, enthält der Gesetzentwurf in Teil 3 auch Regelungen, die diese Richtlinie umsetzen. Die weitere Umsetzung der Richtlinie (EU) 2016/680 wird darüber hinaus gesondert im Fachrecht erfolgen.

Daneben gibt es Bereiche, die nicht dem Anwendungsbereich des EU-Rechts unterfallen, für die bisher neben dem bereichsspezifischen Recht auch das allgemeine Datenschutzrecht Anwendung gefunden hat. Aufgrund der Anpassungen des allgemeinen Rechts an die EU-Datenschutzreform bedarf es auch bezüglich dieser Bereiche anpassender Regelungen.

Auch ist das bereichsspezifische Datenschutzrecht an die Vorgaben der europäischen Datenschutzreform anzupassen, sodass es nicht nur einer Überarbeitung des bisherigen Datenschutzgesetzes NRW (DSG NRW) bedarf, sondern auch der Anpassung weiterer Gesetze mit datenschutzrechtlichem Bezug.

Datum des Originals: 20.02.2018/Ausgegeben: 27.02.2018

B Lösung

Die Anpassung des nordrhein-westfälischen Datenschutzrechts an die europäische Datenschutzreform bedarf einer vollkommenen Neugestaltung des DSG NRW.

Auf Grund des Anwendungsvorrangs des Unionsrechts werden die Regelungen im DSG NRW für den Bereich der Verordnung (EU) 2016/679 (Teil 1 und 2) zukünftig nur noch die Regelungen der Verordnung (EU) 2016/679 ergänzen. Wesentliche datenschutzrechtliche Bestimmungen ergeben sich zukünftig direkt aus der Verordnung (EU) 2016/679. Nach der allgemeinen unionsrechtlichen Vorgabe für Rechtsakte in Verordnungsform ist selbst eine Wiederholung des Verordnungstextes nur in begrenzten Ausnahmefällen zulässig. Im DSG NRW können nur noch dort Regelungen getroffen werden, wo die Verordnung (EU) 2016/679 Regelungsaufträge oder -spielräume lässt. Wo die Verordnung (EU) 2016/679 jedoch Regelungsspielräume lässt, soll das bisherige Datenschutzniveau des Landes Nordrhein-Westfalen aufrechterhalten werden.

Da es Ziel dieses Gesetzentwurfes ist, einen möglichst einheitlichen Rechtsrahmen zu schaffen, der von allen öffentlichen Stellen in gleichem Maße zu beachten ist, sieht er vor, dass (soweit möglich) sowohl für den Anwendungsbereich der Verordnung (EU) 2016/679 als auch für den Anwendungsbereich der Richtlinie (EU) 2016/680 in Teilen die gleichen materiellen und formellen Regelungen gelten. Dies soll durch punktuelle Verweise im Teil 3 auf die Regelungen der Verordnung (EU) 2016/679 geschehen. Wo die Richtlinie (EU) 2016/680 von der Verordnung (EU) 2016/679 abweichende Vorgaben macht, werden im Teil 3 des DSG NRW eigene Regelungen für den Bereich der Richtlinie (EU) 2016/680 geschaffen.

Der Gesetzentwurf enthält in Artikel 1 eine Neufassung des Datenschutzgesetzes Nordrhein-Westfalen mit den Regelungsschwerpunkten:

1. Gemeinsame Bestimmungen für den Regelungsbereich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 insbesondere zur Sicherstellung des Datenschutzes und zur Zulässigkeit der Verarbeitung personenbezogener Daten.

2. Durchführungsbestimmungen zur Verordnung (EU) 2016/679 mit folgenden Schwerpunkten:

   - Der Anwendungsbereich der Verordnung (EU) 2016/679 wird im Interesse eines einheitlichen Datenschutzniveaus auf alle bisher dem DSG NRW a.F. unterstehenden öffentlichen Stellen erstreckt, auch wenn deren Tätigkeit nicht originär dem Anwendungsbereich der Verordnung (EU) 2016/679 unterfällt (§ 4 Absatz 6). Abweichende Regelungen im bereichsspezifischen Recht bleiben möglich.

   - Es werden Regelungen getroffen, unter welchen Voraussetzungen die Rechte der betroffenen Person auf Information, Auskunft, Benachrichtigung und Löschung beschränkt werden dürfen (Teil 2, Kapitel III).

   - Die Regelungsaufträge und -spielräume der Verordnung (EU) 2016/679 zu den besonderen Verarbeitungssituationen im Anwendungsbereich der Verordnung (EU) 2016/679 werden in Teil 2, Kapitel IV ausgestaltet.

   - Die Regelungsspielräume der Verordnung (EU) 2016/679 zu den Pflichten des Verantwortlichen werden in Teil 2, Kapitel V ausgestaltet.

- Die Regelungsaufträge der Verordnung (EU) 2016/679 zur Unabhängigkeit, Tätigkeit und zu den Befugnissen der Aufsichtsbehörde werden in Teil 2, Kapitel VI umgesetzt.

- In Teil 2, Kapitel VII werden Regelungen zu den Straf- und Bußgeldvorschriften getroffen.

3. Umsetzung der Richtlinie (EU) 2016/680 mit den folgenden Schwerpunkten:

   - In Teil 3, Kapitel II werden die Grundsätze der Datenverarbeitung im Anwendungsbereich der Richtlinie geregelt.

   - Teil 3, Kapitel III gestaltet die Rechte der Betroffenen näher aus.

   - Es werden in Teil 3, Kapitel IV Regelungen zu den Pflichten der Verantwortlichen und Auftragsverarbeiter getroffen.

   - In Teil 3, Kapitel V werden Regelungen zu der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit getroffen, soweit diese von den Vorschriften der Verordnung (EU) 2016/679 und Teil 2 abweichen.

   - In Teil 3, Kapitel VI wird die Datenübermittlung an Drittstaaten und internationale Organisationen geregelt.

In Artikel 2 bis 10 werden weitere bereichsspezifische Datenschutzbestimmungen aus Gesetzen aus dem Zuständigkeitsbereich des Ministeriums des Innern an die Vorgaben der europäischen Datenschutzreform angepasst.

C Alternativen

Keine

D Kosten

Durch die Einführung der Datenschutz-Folgenabschätzung sowie die gegenüber der bisherigen Rechtslage erweiterten Pflichten des Verantwortlichen gegenüber dem Betroffenen werden in der Verwaltung voraussichtlich höhere Kosten entstehen. Diese sind jedoch durch die Verordnung (EU) 2016/679 selbst und nicht durch den vorliegenden Gesetzentwurf veranlasst. Der Gesetzentwurf versucht - soweit möglich - unter Ausfüllung der bestehenden Regelungsspielräume das bewährte Datenschutzniveau und damit auch die aktuellen Verwaltungsstrukturen zu erhalten und keine zusätzlichen Pflichten für die Verantwortlichen zu begründen.

Der durch die Verordnung (EU) 2016/679 ausgelöste höhere Beratungsbedarf sowie der daraus resultierende Aufgabenzuwachs bei der Landesbeauftragten für Datenschutz und Informationsfreiheit schließt nicht aus, dass zu den bisherigen in diesem Zusammenhang erfolgten Personalaufstockungen gegebenenfalls langfristig weiterer Personalbedarf entstehen kann. Der konkrete Personalbedarf und die daraus resultierenden Kosten bei der Landesbeauftragten für Datenschutz und Informationsfreiheit können zum jetzigen Zeitpunkt nicht beziffert werden.

Gleiches gilt für den Bereich der Datenschutz-Richtlinie für die Bereiche der Polizei und Justiz. Auch dort müssen - durch die Richtlinie ausgelöst - verbindliche Mindeststandards durch diesen Gesetzentwurf umgesetzt werden, die einen erhöhten Personal- und Sachkostenbedarf zur Folge haben können.

E Zuständigkeit

Zuständig innerhalb der Landesregierung ist das Ministerium des Innern. Beteiligt sind die Staatskanzlei sowie alle Ressorts der Landesregierung.

F Auswirkungen auf die Selbstverwaltung und die Finanzlage der Gemeinden und Gemeindeverbände

Ebenso wie die voraussichtlich höheren Kosten für die Verwaltung zur Erfüllung der Pflichten aus der Verordnung (EU) 2016/679 entstehen auch für die Gemeinden voraussichtlich diese Kosten. Auch in diesem Fall entstehen die Kosten jedoch aus der Verordnung (EU) 2016/679 selbst und nicht aus dem hiesigen Gesetzentwurf.

G Finanzielle Auswirkungen auf die Unternehmen und die privaten Haushalte

Da der Bund die Gesetzgebungskompetenz für den Bereich des Datenschutzes im nicht-öffentlichen Bereich hat, entstehen durch diesen Gesetzentwurf keine neuen Kosten für Unternehmen und private Haushalte, da er keine datenschutzrechtlichen Vorschriften für Unternehmen und private Haushalte zum Inhalt hat.

H Geschlechterdifferenzierte Betrachtung der Auswirkungen des Gesetzes

Bei den vorgesehenen Maßnahmen wird nicht nach dem Geschlecht unterschieden.

I Auswirkungen auf die nachhaltige Entwicklung (im Sinne der Nachhaltigkeitsstrategie NRW)

Die Nachhaltigkeitspostulate werden vom vorliegenden Gesetzentwurf nicht berührt. Konflikte mit der Nachhaltigkeitsstrategie NRW bestehen nicht.

J Befristung

Eine Befristung des Artikelgesetzes ist nicht vorgesehen, da die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 keine Befristung vorsehen.

G e g e n ü b e r s t e l l u n g

Gesetzentwurf der Landesregierung

Auszug aus den geltenden Gesetzesbestimmungen

Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU)

Artikel 1
Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)

Inhaltsübersicht
Teil 1 Allgemeine Bestimmungen

Teil 2
Durchführungsbestimmungen zur Verordnung (EU) 2016/679

Kapitel 1
Grundsätze der Verarbeitung personenbezogener Daten

Kapitel 2
Rechte der betroffenen Personen

Kapitel 3
Rechte der betroffenen Personen

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

Kapitel 5
Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

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 Auf-

wand 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.

§ 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) Für den Landtag gelten die Verordnung (EU) 2016/679 und Teil 2 dieses Gesetzes, soweit er Verwaltungsaufgaben wahrnimmt.

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

(4) 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 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.

(5) 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.

(6) 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. Im Fall der entsprechenden Anwendung sind die Vorschriften über den gerichtlichen Rechtsschutz nach

§ 20 des Bundesdatenschutzgesetzes anzuwenden.

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 nur 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

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.

§ 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.

(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 oder
4. die Verarbeitung zu Ausbildungs- und Prüfungszwecken erfolgen soll, sofern berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen.

(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 übermittelten personenbezogenen Daten dürfen nur für die Zwecke verarbeitet werden, zu denen sie übermittelt wurden. Hierauf ist in den Fällen der Absätze 1, 2 und 4 bei der Übermittlung an nicht-öffentliche Stellen hinzuweisen.

(7) 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 und

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.

(2) Die Auskunftserteilung kann abgelehnt werden, soweit und solange

1. dies zur Verfolgung von Straftaten, Ordnungswidrigkeiten und 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 Wah-

rung 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 einschließlich solcher im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken soll in anonymisierter Form erfolgen. Stehen einer Anonymisierung wissenschaftliche Gründe entgegen, dürfen die Daten auch verarbeitet werden, wenn sie pseudonymisiert werden und der mit der Forschung befasste Personenkreis oder die empfangende Stelle oder Person keinen Zugriff auf die Zuordnungsfunktion hat. Datenerfassung, Anonymisierung oder Pseudonymisierung kann auch durch die mit der Forschung befassten Personen erfolgen, wenn sie zuvor nach dem Verpflichtungsgesetz zur Verschwiegenheit verpflichtet worden sind und unter der Aufsicht der übermittelnden Stelle stehen.

(2) Ist eine Anonymisierung oder Pseudonymisierung nicht möglich, so ist die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken ohne Einwilligung in Ergänzung zu Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 auch dann rechtmäßig, wenn

1. schutzwürdige Belange der betroffenen Person wegen der Art der Daten oder der Art der Verwendung nicht beeinträchtigt werden oder
2. der Zweck, der auf andere Weise nicht oder nur mit unverhältnismäßig großem Aufwand erreicht werden kann, und das öffentliche Interesse an der Durchführung des Forschungs- oder Statistikvorhabens die schutzwürdigen Belange der betroffenen Person überwiegen.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Zuvor sind die Merkmale gesondert zu spei-

chern, 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.

(6) Eine Übermittlung personenbezogener Daten an Empfänger, für die dieses Gesetz keine Anwendung findet, ist zulässig, wenn sich die Empfänger verpflichten, die Daten nur für das von ihnen zu bezeichnende Forschungs- oder Statistikvorhaben und nach Maßgabe der Absätze 1 bis 3 zu verarbeiten und jederzeit Kontrollen durch die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu ermöglichen. Bei einer Datenübermittlung an Stellen außerhalb des

Geltungsbereichs dieses Gesetzes hat die übermittelnde Stelle die für den Empfänger zuständige Datenschutzkontrollbehörde zu unterrichten.

§ 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 Erfüllung der Aufgaben öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts,
3. zum Schutz des Eigentums oder Besitzes oder
4. 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, spätestens jedoch vier Wochen nach ihrer Erhebung, 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 6 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 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 4 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 Per-

son 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 4 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 Ge-

sundheit 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 beabsichtig-

ten 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. den Namen und die Kontaktdaten des Verantwortlichen und der oder 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 übermittel-

ten 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.

Artikel 2
Änderung des Informationsfreiheitsgesetzes Nordrhein-Westfalen

Das Informationsfreiheitsgesetz Nordrhein-Westfalen vom 27. November 2001 (GV. NRW. S. 806), das zuletzt durch Artikel 4 des Gesetzes vom 2. Oktober 2014 (GV. NRW. S. 622) geändert worden ist, wird wie folgt geändert:

1. In § 10 Absatz 2 werden die Wörter „gemäß § 4 Abs. 6 des Datenschutzgesetzes Nordrhein-Westfalen“ durch die Wörter „nach dem geltenden Datenschutzrecht“ ersetzt.

Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz Nordrhein-Westfalen - IFG NRW)

§ 10
Einwilligung der betroffenen Person

(1) Im Fall des § 9 Abs. 1 Buchstabe a) ist zu prüfen, ob dem Antrag auf Informationszugang nach Abtrennung oder Schwärzung der personenbezogenen Daten stattgegeben werden kann. Ist dies nicht oder nur mit unverhältnismäßigem Aufwand möglich, hat die öffentliche Stelle unverzüglich die Einwilligung der betroffenen Person einzuholen. Wird die Einwilligung nicht erteilt oder gilt sie nach § 5 Abs. 3 als verweigert, besteht der Anspruch auf Informationszugang nicht.

(2) Die öffentlichen Stellen treffen gemäß § 4 Abs. 6 des Datenschutzgesetzes Nordrhein-Westfalen geeignete Maßnahmen, damit Informationen, die dem Anwendungsbereich der §§ 6 bis 9 unterfallen, möglichst ohne unverhältnismäßigen Aufwand abgetrennt werden können.

2. § 13 wird wie folgt gefasst:

„§ 13 Beauftragte oder Beauftragter für das Recht auf Information	§ 13 Beauftragte oder Beauftragter für das Recht auf Information
(1) Für die Sicherstellung des Rechts auf Information ist die oder der Landesbeauftragte für den Datenschutz und Informationsfreiheit zuständig.	(1) Für die Sicherstellung des Rechts auf Information ist die oder der Landesbeauftragte für den Datenschutz zuständig.
(2) Jeder hat das Recht, die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit als Beauftragte oder Beauftragten für das Recht auf Information anzurufen.	(2) Jeder hat das Recht, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz als Beauftragte oder Beauftragten für das Recht auf Information anzurufen. Das Datenschutzgesetz Nordrhein-Westfalen gilt entsprechend.
(3) Berufung und Rechtsstellung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit richtet sich nach § 25 des Datenschutzgesetzes Nordrhein-Westfalen vom [einsetzen: Ausfertigungsdatum und Fundstelle des neuen Datenschutzgesetzes].	(3) Die oder der Landesbeauftragte für den Datenschutz legt dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über ihre oder seine Tätigkeit als Beauftragte oder Beauftragter für das Recht auf Information vor. § 27 des Datenschutzgesetzes Nordrhein-Westfalen gilt entsprechend.
(4) Die in § 2 vom Anwendungsbereich umfassten Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit bei der Aufgabenerfüllung zu unterstützen. Der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist dabei insbesondere 1. Auskunft zu ihren oder seinen Fragen zu erteilen sowie die Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit dem Informationsanliegen stehen und 2. Zutritt zu Diensträumen zu gewähren. Gesetzliche Geheimhaltungsvorschriften können einem Auskunfts- oder Einsichtsverlangen nicht entgegen gehalten werden.	

(5) Die Rechte der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nach Absatz 4 und 5 dürfen nur von ihr oder ihm persönlich ausgeübt werden, wenn die oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet. 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.

(6) Stellt die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit Verstöße gegen dieses Gesetz bei nach § 2 informationspflichtigen Stellen fest, so fordert sie oder er diese zur Mängelbeseitigung auf. Bei Verstößen gegen die Informationspflicht kann er oder sie diese beanstanden

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

und fordert zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nummer 2 bis 5 unterrichtet die oder der Landesbeauftragte für Daten-

schutz und Informationsfreiheit gleichzeitig auch die zuständige Aufsichtsbehörde.

(7) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt oder wenn ihre Behebung sichergestellt ist.

(8) Mit der Beanstandung kann die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Informationszugangs verbinden.

(9) Die gemäß Absatz 7 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die in Absatz 7 Nummer 2 bis 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu.

(10) Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit legt dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über ihre oder seine Tätigkeit als Beauftragte oder Beauftragter für das Recht auf Information vor. § 30 des Datenschutzgesetzes Nordrhein-Westfalen gilt entsprechend.“

Artikel 3
Änderung des Meldegesetzes NRW

Das Meldegesetz NRW in der Fassung der Bekanntmachung vom 16. September 1997 (GV. NRW. S. 332; ber. S. 386), das zuletzt durch Artikel 1 des Gesetzes vom 8. September 2015 (GV. NRW. S. 666) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 2 wie folgt gefasst:

   „§ 2 Verarbeiten von Daten“.

2. § 2 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

„§ 2
Verarbeiten von Daten“.

Meldegesetzes für das
Land Nordrhein-Westfalen
(Meldegesetz NRW - MG NRW)

Inhaltsübersicht

§ 2 Speicherung und Nutzung von Daten

§ 2
Speicherung und Nutzung von Daten

(1) Über die in § 3 des Bundesmeldegesetzes vom 3. Mai 2013 (BGBl. I S. 1084) in der jeweils geltenden Fassung aufgeführten Daten hinaus speichern die Meldebehörden folgende Daten der wohnhaften Person (Einwohner/Einwohnerin) einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise im Melderegister:

1. die Tatsache, dass für die Einwohnerin oder den Einwohner ein Untersuchungsberechtigungsschein ausgestellt worden ist, im Rahmen der Mitwirkung bei der Erfüllung von Aufgaben nach dem Jugendarbeitsschutzgesetz vom 12. April 1976 (BGBl. I S. 965), das zuletzt durch Artikel 2 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10) geändert worden ist,
2. die Tatsache, dass die Einwohnerin oder der Einwohner als gefördert geltenden Wohnraum im Sinne des § 1 des Gesetzes zur Förderung und Nutzung von Wohnraum für das Land Nordrhein-Westfalen vom 8. Dezember 2009 (GV. NRW. S. 772), das zuletzt durch Artikel 1 des Gesetzes vom 10. April 2014 (GV. NRW. S. 269) geändert worden ist, bewohnt, im Rahmen der Mitwirkung bei der Erfüllung von

Aufgaben nach dem Gesetz zur Förderung und Nutzung von Wohnraum für das Land Nordrhein-Westfalen, und

3. Daten über Zeiten im Reichsarbeitsdienst, der Wehrmacht oder in Kriegsgefangenschaft für die Geltendmachung von Rentenansprüchen als Nachweis für die Einwohnerin oder den Einwohner, soweit diese Daten bei der Meldebehörde vor Inkrafttreten dieses Gesetzes gespeichert gewesen sind.

(2) Die Meldebehörde darf, auch gegen Kostenerstattung, unter den Voraussetzungen des § 46 Absatz 1 des Bundesmeldegesetzes die dort genannten Daten für die Versendung von Einladungen oder anderen Unterlagen an die Betroffenen nutzen, wenn dies zur Erreichung des mit der Gruppenauskunft beabsichtigten Zweckes genügt und die Weitergabe an Dritte nicht erforderlich ist.

b) In Absatz 2 wird das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.

3. Dem § 7 Absatz 1 wird folgender Satz angefügt:

§ 7
Verfahren des automatisierten Abrufs durch Behörden

(1) Das Bereithalten von Daten zum automatisierten Abruf erfolgt durch die Meldebehörden für alle öffentlichen Stellen des Landes Nordrhein-Westfalen, die der Aufsicht des Landes unterstehen, und für die Gerichte über das von dem für Inneres zuständigen Ministerium betriebene Meldeportal Behörden.

„Die Zulässigkeit ergibt sich aus § 6 Absatz 1 des Datenschutzgesetzes Nordrhein-Westfalen vom [einsetzen: Ausfertigungsdatum und Fundstelle des neuen Datenschutzgesetzes] in Verbindung mit Artikel 6 Absatz 1 Buchstaben c und e der Verordnung (EU) 2016/679“.

(2) Das Meldeportal Behörden ist zentrale Stelle für den automatisierten Abruf durch andere öffentliche Stellen nach den §§ 38 und 39 des Bundesmeldegesetzes, wenn diese zu Abrufen von Meldedaten von dem für Inneres zuständigen Ministerium des Landes Nordrhein-Westfalen oder der zuständigen Stelle eines anderen Landes zugelassen worden sind.

(3) Die Meldebehörden sind zum Anschluss an das Meldeportal Behörden verpflichtet. Die Meldebehörden sind nicht verpflichtet, den automatisierten Abruf auf anderem Weg bereit zu halten, sofern ein Abruf über das Meldeportal Behörden eröffnet ist oder eröffnet werden könnte.

Artikel 4
Änderung des Ausführungsgesetzes NRW Glücksspielstaatsvertrag

§ 12 Absatz 5 des Ausführungsgesetzes NRW Glücksspielstaatsvertrag vom 13. November 2012 (GV. NRW. S. 524) wird wie folgt gefasst:

Gesetz zur Ausführung des Glücksspielstaatsvertrages (Ausführungsgesetz NRW Glücksspielstaatsvertrag - AG GlüStV NRW)

§ 12
Mitwirkung am übergreifenden Sperrsystem

(1) Die Veranstalter von Glücksspielen nach § 3 Absatz 1 in Nordrhein-Westfalen sind verpflichtet, Spielersperren im Sinne des § 8 Glücksspielstaatsvertrag sowie deren Änderungen und Aufhebungen unverzüglich zur Aufnahme in die Sperrdatei nach § 23 Absatz 1 Satz 1 Glücksspielstaatsvertrag zu übermitteln. Gesperrte Spieler dürfen an Wetten und an Lotterien, die häufiger als zweimal pro Woche veranstaltet werden, nicht teilnehmen.

(2) Im Fall der Fremdsperre ist der betroffene Spieler vor Eintrag in das übergreifende Sperrsystem anzuhören. Stimmt er der Fremdsperre nicht zu, sind die der Fremdsperre zugrundeliegenden Tatsachen durch geeignete Maßnahmen zu überprüfen.

(3) Vermittler von öffentlichen Glücksspielen sind gemäß § 8 Absatz 6 Glücksspielstaatsvertrag verpflichtet am übergreifenden Sperrsystem nach § 23 Glücksspielstaatsvertrag mitzuwirken.

(4) Veranstalter und Vermittler haben nach Maßgabe des Glücksspielstaatsvertrages die Daten mit der Sperrdatei abzugleichen, soweit sie nach § 4 Absatz 1 Satz 1 Nummer 7 und 8 am Sperrsystem teilnehmen.

„(5) Verantwortlicher für die Daten gesperrter Spielerinnen oder Spieler in der Sperrdatei im Sinne des Artikel 4 Nummer 7 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) ist die nach § 23 Absatz 1 Satz 1 des Glücksspielstaatsvertrags zuständige Behörde."

Artikel 5
Änderung des Spielbankgesetzes NRW

§ 6 Absatz 8 des Spielbankgesetzes NRW vom 13. November 2012 (GV. NRW. S. 524) wird wie folgt gefasst:

(5) Verantwortliche Stelle im Sinne des § 3 Absatz 7 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814), für die Daten gesperrter Spieler ist diejenige Stelle, die die Sperre ausgesprochen hat und die nach § 23 Absatz 1 Satz 1 Glücksspielstaatsvertrag zuständige Behörde.
Die Daten gesperrter Spieler dürfen nur für die Kontrolle der Spielersperre verwendet werden.

(6) Die allgemeinen Auskunftsrechte gesperrter Spieler nach § 34 Bundesdatenschutzgesetz bleiben unberührt.

Gesetz über die Zulassung öffentlicher Spielbanken im Land Nordrhein-Westfalen (Spielbankgesetz NRW - SpielbG NRW)

§ 6
Spielersperre

(1) Gesperrte Spieler dürfen nach Maßgabe des § 20 Absatz 2 Glücksspielstaatsvertrag am Spielbetrieb in Spielbanken nicht teilnehmen. Zur Feststellung einer Spielersperre bedienen sich die Spielbanken der Sperrdatei der nach § 23 Absatz 1 Satz 1 Glücksspielstaatsvertrag zuständigen Behörde. § 21 Absatz 3 AG Glücksspielstaatsvertrag NRW gilt entsprechend.

(2) Die Spielbanken sperren Personen, die dies beantragen (Selbstsperre) oder von denen sie auf Grund der Wahrnehmung ihres Personals oder auf Grund von Meldungen Dritter wissen oder auf Grund sonstiger tatsächlicher Anhaltspunkte annehmen müssen, dass sie spielsuchtgefährdet, spielsüchtig oder überschuldet sind, ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre).

(3) Die Spielbanken können Personen sperren, die gegen die Spielordnung (§ 10) oder die Spielregeln verstoßen, gegen die ein begründeter Verdacht eines solchen Verstoßes besteht oder denen auf Grund des Hausrechts der Zutritt zur Spielbank untersagt wurde (Störersperre). Die Tatsachen, die zur Sperre geführt haben, sind zu speichern. Die Absätze 7 und 9 gelten entsprechend.

(4) Die Spielbanken sind verpflichtet, die Spielersperren nach Absatz 2 sowie deren Änderungen und Aufhebungen unverzüglich an die nach § 23 Absatz 1 Satz 1 Glücksspielstaatsvertrag zuständige Behörde zur Aufnahme in die Sperrdatei zu übermitteln.

(5) Im Fall der Fremdsperre ist der betroffene Spieler vor Eintrag in das übergreifende Sperrsystem anzuhören. Stimmt er der Fremdsperre nicht zu, sind die der Fremdsperre zugrundeliegenden Tatsachen durch geeignete Maßnahmen zu überprüfen.

(6) Die Selbstsperre und die Fremdsperre betragen mindestens ein Jahr. Nach Einrichtung der Sperre teilt die Spielbank dem betroffenen Spieler Art und Dauer der Sperre unverzüglich schriftlich mit.

(7) Die Spielbank entscheidet auf Antrag des gesperrten Spielers nach Ablauf der in Absatz 6 Satz1 bestimmten Frist über die Aufhebung der Sperre. Der gesperrte Spieler hat einen Anspruch auf Löschung der Spielersperre, wenn die Gründe, die zur Eintragung in die Sperrdatei geführt haben, nicht mehr gegeben sind.

„(8) Verantwortlicher für die Daten gesperrter Spielerinnen oder Spieler in der Sperrdatei im Sinne des Artikel 4 Nummer 7 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) ist die nach § 23 Absatz 1 Satz 1 des Glücksspielstaatsvertrags zuständige Behörde.“

(8) Verantwortliche Stelle im Sinne des § 3 Absatz 7 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814), für die Daten gesperrter Spieler ist diejenige Stelle, die die Sperre ausgesprochen hat und die nach § 23 Absatz 1 Satz 1 Glücksspielstaatsvertrag zuständige Behörde.

(9) Die allgemeinen Auskunftsrechte gesperrter Spieler nach § 34 Bundesdatenschutzgesetz bleiben unberührt.

Artikel 6
Änderung des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen

Das Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 12. November 1999 (GV. NRW. S. 602), das zuletzt durch Artikel 8 des Gesetzes vom [einsetzen: Ausfertigungsdatum und Fundstelle des Gesetzes zum Abbau unnötiger und belastender Vorschriften im Land Nordrhein-Westfalen - Entfesselungspaket I] geändert worden ist, wird wie folgt geändert:

Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen (VwVfG NRW)

1. In der Inhaltsübersicht werden in der Angabe zu § 3b die Wörter „Personenbezogene Daten," gestrichen.

3b Personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse

2. § 3b wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

„§ 3b
Betriebs- und Geschäftsgeheimnisse"

   b) § 3b Satz 2 wird aufgehoben.

§ 3b
Personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse

Die Behörde darf Angaben über persönliche und sachliche Verhältnisse einer natürlichen Person sowie Betriebs- oder Geschäftsgeheimnisse nicht unbefugt offenbaren. Sie unterliegt, soweit sie personenbezogene Daten verarbeitet, den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen.

§ 26
Beweismittel

(1) Die Behörde bedient sich unter Beachtung des § 3b der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere

1. Auskünfte jeder Art einholen,
2. Beteiligte anhören, Zeugen und Sachverständige vernehmen oder die schriftliche oder elektronische Äußerung von Beteiligten, Sachverständigen und Zeugen einholen,
3. Urkunden und Akten beiziehen,
4. den Augenschein einnehmen.

3. In § 26 Absatz 2 Satz 3 werden die Wörter „ , zur Angabe von personenbezogenen Daten oder von Betriebs- und Geschäftsgeheimnissen“ gestrichen.

(2) Die Beteiligten sollen bei der Ermittlung des Sachverhalts mitwirken. Sie sollen insbesondere ihnen bekannte Tatsachen und Beweismittel angeben. Eine weitergehende Pflicht, bei der Ermittlung des Sachverhalts mitzuwirken, insbesondere eine Pflicht zum persönlichen Erscheinen, zur Angabe von personenbezogenen Daten oder von Betriebs- und Geschäftsgeheimnissen oder zur Aussage, besteht nur, soweit sie durch Rechtsvorschrift besonders vorgesehen ist. Der Auskunftspflichtige kann die Auskunft auf solche Fragen, zu deren Beantwortung er durch Rechtsvorschrift verpflichtet ist, verweigern, wenn deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nrn. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

(3) Für Zeugen und Sachverständige besteht eine Pflicht zur Aussage oder zur Erstattung von Gutachten, wenn sie durch Rechtsvorschrift vorgesehen ist. Falls die Behörde Zeugen und Sachverständige herangezogen hat, erhalten sie auf Antrag in entsprechender Anwendung des Justizvergütungs- und -entschädigungsgesetzes eine Entschädigung oder Vergütung.

Artikel 7
Änderung des Landesbeamtengesetzes

Das Landesbeamtengesetz vom 14. Juni 2016 (GV. NRW. S. 310, ber. S. 642), das zuletzt durch Artikel 1 des Gesetzes vom 19. September 2017 (GV. NRW. S. 764) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden die Angaben zu den §§ 86 und 87 wie folgt gefasst:

„§ 86 Auskunftsrecht
§ 87 Übermittlung an Behörden und Auskunft an nicht betroffene Personen“.

Gesetz über die Beamtinnen und Beamten des Landes Nordrhein-Westfalen (Landesbeamtengesetz - LBG NRW)

§ 86 Akteneinsicht
§ 87 Vorlage und Auskunft

2. § 83 wird wie folgt geändert:

a) In Absatz 1 Satz 2 und 7 wird jeweils das Wort „automatisiert" durch die Wörter „im Wege des automatisierten Verfahrens“ ersetzt.

§ 83
Personalakten - allgemein

(1) Für jede Beamtin und jeden Beamten ist eine Personalakte zu führen. Sie kann in Teilen oder vollständig automatisiert geführt werden. Die Personalakte kann nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert werden. Teilakten können bei der für den betreffenden Aufgabenbereich zuständigen Behörde geführt werden. Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für die Beamtin oder den Beamten zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. In die Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen. Wird die Personalakte nicht in Schriftform oder vollständig automatisiert geführt, legt die personalverwaltende Stelle jeweils schriftlich fest, welche Teile in welcher Form geführt werden und nimmt dies in das Verzeichnis nach Satz 6 auf.

(2) Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren. Satz 1 gilt entsprechend für Beauftragte des Dienstherrn, soweit sie zur Wahrnehmung besonderer Belange an Personalentscheidungen zu beteiligen sind. Zugang zur Personalakte haben ferner die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse andernfalls nur mit unverhältnismäßigem Aufwand oder unter Gefährdung des Prüfzwecks gewinnen könnten.

(3) Nicht Bestandteil der Personalakte sind Unterlagen, die besonderen, von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, insbesondere Prüfungs-, Sicherheits- und Kindergeldakten. Kindergeldakten können mit Besoldungs- und Versorgungsakten verbunden geführt werden, wenn diese von der übrigen Personalakte getrennt sind und von einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden. § 35 des Ersten Buches Sozialgesetzbuch -Allgemeiner Teil- (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015) in der jeweils geltenden Fassung und die §§ 67 bis 78 des Zehnten Buches Sozialgesetzbuch -Sozialverwaltungsverfahren und Sozialdatenschutz- in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130) in der jeweils geltenden Fassung bleiben unberührt.

b) Absatz 4 Satz 1 wird wie folgt gefasst:

„Der Dienstherr darf personenbezogene Daten über Bewerberinnen und Bewerber, Beamtinnen und Beamte und ehemalige Beamtinnen und Beamte verarbeiten, soweit dies im Rahmen der Personalverwaltung und der Personalwirtschaft zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist oder eine Rechtsvorschrift dies erlaubt.“

(4) Der Dienstherr darf personenbezogene Daten über Bewerberinnen und Bewerber, Beamtinnen und Beamte und ehemalige Beamtinnen und Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen der Genehmigung durch die zuständige oberste Dienstbehörde.

	§ 84 **Beihilfeakten**
3. In § 84 werden in Satz 4 die Wörter „Die Beihilfeakte darf“ durch die Wörter „Beihilfedaten dürfen“ und das Wort „weitergegeben“ durch das Wort „übermittelt“ ersetzt.	Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Die Beihilfeakte darf für andere als für Beihilfezwecke nur verwendet oder weitergegeben werden, wenn die oder der Beihilfeberechtigte und die oder der bei der Beihilfegewährung berücksichtigte Angehörige im Einzelfall einwilligen, die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Die Sätze 1 bis 4 gelten entsprechend für Unterlagen über Heilfürsorge und Heilverfahren.
4. § 86 wird wie folgt gefasst:	
„**§ 86** **Auskunftsrecht**	**§ 86** **Akteneinsicht**
(1) Der Anspruch der Beamtinnen und Beamten auf Auskunft aus ihren Personalakten oder aus anderen Akten, die personenbezogene Daten über sie enthalten und für ihr Dienstverhältnis verarbeitet werden, umfasst auch die Gewährung von Akteneinsicht, soweit gesetzlich nichts anderes bestimmt ist. Beamtinnen und Beamte haben, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in ihre vollständige Personalakte. Die Auskunft aus Sicherheitsakten ist unzulässig. Unzulässig ist die Einsichtnahme in Daten der oder des Betroffenen, die mit Daten Dritter oder geheimhaltungsbedürftigen nichtpersonenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist.	(1) Die Beamtin oder der Beamte hat, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständige Personalakte.

(2) Einer oder einem Bevollmächtigten der Beamtin oder des Beamten ist Auskunft zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene und deren Bevollmächtigte, wenn ein berechtigtes Interesse glaubhaft gemacht wird.

(3) Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Soweit wichtige dienstliche Gründe nicht entgegenstehen, werden Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt. Der Beamtin oder dem Beamten ist auf Verlangen ein Ausdruck der zu ihrer oder seiner Person automatisiert gespeicherten Personalaktendaten zu überlassen.“

(2) Einer oder einem Bevollmächtigten der Beamtin oder des Beamten ist Einsicht zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene, wenn ein berechtigtes Interesse glaubhaft gemacht wird, und deren Bevollmächtigte. Für Auskünfte aus der Personalakte gelten die Sätze 1 und 2 entsprechend.

(3) Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Soweit dienstliche Gründe nicht entgegenstehen, können Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden; der Beamtin oder dem Beamten ist auf Verlangen ein Ausdruck der zu ihrer oder seiner Person automatisiert gespeicherten Personalaktendaten zu überlassen.

(4) Die Beamtin oder der Beamte hat ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über sie oder ihn enthalten und für ihr oder sein Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist; dies gilt nicht für Sicherheitsakten. Die Einsichtnahme ist unzulässig, wenn die Daten der oder des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nichtpersonenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist der Beamtin oder dem Beamten Auskunft zu erteilen.

5. § 87 wird wie folgt gefasst:

„**§ 87**
Übermittlung an Behörden und Auskunft an nicht betroffene Personen

(1) Ohne Einwilligung der Beamtin oder des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde zu übermitteln. Das Gleiche gilt für Behörden im Bereich desselben Dienstherrn, soweit die Übermittlung der Akte zur Vorbereitung oder Durchführung einer Personalentschei-

§ 87
Vorlage und Auskunft

(1) Ohne Einwilligung der Beamtin oder des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das Gleiche gilt für Behörden im Bereich desselben Dienstherrn, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. Ärztinnen und Ärzten, die im Auftrag der personalverwal-

dung notwendig ist. Ärztinnen und Ärzten, die im Auftrag der personalverwaltenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung übermittelt werden. Für Auskünfte aus der Personalakte gelten die Sätze 1 bis 3 entsprechend. Soweit eine Auskunft ausreicht, ist von einer Übermittlung abzusehen.

tenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden. Für Auskünfte aus der Personalakte gelten die Sätze 1 bis 3 entsprechend. Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen.

(2) Auskünfte an nicht betroffene Personen dürfen nur mit Einwilligung der Beamtin oder des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen der nicht betroffenen Person die Auskunftserteilung zwingend erfordert. Inhalt und Empfänger der Auskunft sind der Beamtin oder dem Beamten schriftlich mitzuteilen.

(2) Auskünfte an Dritte dürfen nur mit Einwilligung der Beamtin oder des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen der oder des Dritten die Auskunftserteilung zwingend erfordert. Inhalt und Empfänger der Auskunft sind der Beamtin oder dem Beamten schriftlich mitzuteilen.

(3) Übermittlung und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken."

(3) Vorlage und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken.

6. § 89 wird wie folgt geändert:

§ 89
Verarbeitung und Übermittlung von Personalaktendaten

a) In Absatz 1 Satz 3 werden die Wörter „automatisierter Datenabruf" durch die Wörter „Datenabruf im Wege des automatisierten Verfahrens" ersetzt.

(1) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet werden. Ihre Übermittlung ist nur nach Maßgabe des § 87 zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

b) Absatz 2 wird wie folgt gefasst:

„(2) Personalaktendaten im Sinne des § 84 dürfen im automatisierten Verfahren im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt und nur nach Maßgabe des § 84 sowie im Fall der Übertragung von Aufgaben der Personalverwaltung im Sinne des § 91 verarbeitet werden."

(2) Personalaktendaten im Sinne des § 84 dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet werden.

c) In Absatz 3 wird das Wort „automatisiert" durch die Wörter „im Wege des automatisierten Verfahrens“ ersetzt.

d) In Absatz 4 wird das Wort „automatisierte" gestrichen und nach dem Wort „Daten“ werden die Wörter „im automatisierten Verfahren“ eingefügt.

(3) Von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet werden, soweit sie die Eignung betreffen und ihre Verarbeitung dem Schutz der Beamtin oder des Beamten dient.

(4) Beamtenrechtliche Entscheidungen dürfen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden, die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden.

(5) Bei erstmaliger Speicherung ist der oder dem Betroffenen die Art der über sie oder ihn gemäß Absatz 1 gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist sie oder er zu benachrichtigen. Ferner sind die Verarbeitungsformen automatisierter Personalverwaltungsverfahren zu dokumentieren und einschließlich des jeweiligen Verwendungszweckes sowie der regelmäßigen Empfängerinnen oder Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekanntzugeben.

§ 91
Übertragung von Aufgaben der Personalverwaltung

(1) Der Dienstherr kann Aufgaben der Personalverwaltung zur Durchführung auf eine personalverwaltende Stelle eines anderen Dienstherrn übertragen. Die Aufgabenübertragung kann sich auf die Durchführung von Widerspruchsverfahren und die Vertretung des Dienstherrn in gerichtlichen Verfahren erstrecken. Der Dienstherr darf die zur Aufgabenerfüllung erforderlichen Personalaktendaten an die personalverwaltende Stelle übermitteln.

(2) Die mit der Durchführung beauftragte personalverwaltende Stelle handelt in Vertretung des die Aufgabe übertragenden Dienstherrn.

(3) Für die mit der Durchführung beauftragte personalverwaltende Stelle gelten die Regelungen der §§ 83 bis 90 sowie § 50 des Beamtenstatusgesetzes entsprechend.

(4) Die Absätze 1 bis 3 gelten entsprechend für die Tätigkeit der kommunalen Versorgungskassen gemäß Gesetz über die kommunalen Versorgungskassen und Zusatzversorgungskassen im Land Nordrhein-Westfalen.

7. § 91 Absatz 5 Satz 3 wird wie folgt gefasst:

„Die §§ 84 und 89 Absatz 2 sowie Artikel 28 der Verordnung (EU) 2016/679 gelten entsprechend.“

(5) Der Dienstherr kann sich zur Erfüllung seiner Verpflichtungen im Rahmen der Beihilfebearbeitung nach § 75 auch geeigneter Stellen außerhalb des öffentlichen Dienstes bedienen und diesen die zur Beihilfebearbeitung erforderlichen Daten übermitteln. Die beauftragte Stelle darf die Daten, die ihr im Rahmen der Beihilfebearbeitung bekannt werden, nur für diesen Zweck verarbeiten. §§ 84 und 89 Absatz 2 sowie § 11 des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542) in der jeweils geltenden Fassung gelten entsprechend.

8. § 91a wird wie folgt gefasst:

„**§ 91a**
Verarbeitung von Personalakten im Auftrag

(1) Die Verarbeitung von Personalaktendaten im Auftrag der personalverwaltenden Behörde ist auch außerhalb des öffentliches Dienstes zulässig,

1. soweit sie erforderlich ist für die automatisierte Erledigung von Aufgaben und
2. wenn der Verantwortliche die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragsverarbeiter regelmäßig kontrolliert.

§ 91a
Verarbeitung von Personalakten im Auftrag

(1) Die Verarbeitung von Personalaktendaten im Auftrag der personalverwaltenden Behörde ist auch außerhalb des öffentliches Dienstes zulässig,

1. soweit sie erforderlich ist für die automatisierte Erledigung von Aufgaben, und
2. wenn der Auftraggeber die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragnehmer regelmäßig kontrolliert.

(2) Die Auftragserteilung bedarf der vorherigen Zustimmung der obersten Dienstbehörde. Zu diesem Zweck hat der Verantwortliche der obersten Dienstbehörde rechtzeitig vor der Auftragserteilung schriftlich mitzuteilen:

1. den Auftragsverarbeiter, die von diesem getroffenen technischen und organisatorischen Maßnahmen und die ergänzenden Festlegungen nach Absatz 3,
2. die Aufgabe, zu deren Erfüllung der Auftragsverarbeiter die Daten verarbeiten soll,
3. die Art der Daten, die für den Verantwortlichen verarbeitet werden sollen, und den Kreis der Beschäftigten, auf den sich diese Daten beziehen, sowie
4. die beabsichtigte Erteilung von Unteraufträgen durch den Auftragsverarbeiter.

(3) In dem Auftrag ist insbesondere schriftlich festzulegen:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Datenverarbeitung, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 14 des Datenschutzgesetzes Nordrhein-Westfalen zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten und gegebenenfalls die Vernichtung der Papierakte,
5. die von dem Auftragsverarbeiter vorzunehmenden Kontrollen der Datenverarbeitung, insbesondere die Überprüfung, ob das Ergebnis bildlich und inhaltlich mit der Papierakte übereinstimmt,
6. die Kontrollrechte des Verantwortlichen und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters,

(2) Die Auftragserteilung bedarf der vorherigen Zustimmung der obersten Dienstbehörde. Zu diesem Zweck hat der Auftraggeber der obersten Dienstbehörde rechtzeitig vor der Auftragserteilung schriftlich mitzuteilen:

1. den Auftragnehmer, die von diesem getroffenen technischen und organisatorischen Maßnahmen und die ergänzenden Festlegungen nach Absatz 3,
2. die Aufgabe, zu deren Erfüllung der Auftragnehmer die Daten verarbeiten soll,
3. die Art der Daten, die für den Auftraggeber verarbeitet werden sollen, und den Kreis der Beschäftigten, auf den sich diese Daten beziehen, sowie
4. die beabsichtigte Erteilung von Unteraufträgen durch den Auftragnehmer.

(3) In dem Auftrag ist insbesondere schriftlich festzulegen:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Datenverarbeitung, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 10 des Datenschutzgesetzes Nordrhein-Westfalen zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung, und Sperrung von Daten und gegebenenfalls die Vernichtung der Papierakte,
5. die von dem Auftragnehmer vorzunehmenden Kontrollen der Datenverarbeitung, insbesondere die Überprüfung, ob das Ergebnis bildlich und inhaltlich mit der Papierakte übereinstimmt.
6. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

7. mitzuteilende Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
8. der Umfang der Weisungsbefugnisse, die sich der Verantwortliche gegenüber dem Auftragsverarbeiter vorbehält,
9. die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, und
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragsverarbeiter gespeicherter Daten, sobald diese für die Erfüllung des Auftrags nicht mehr benötigt werden, spätestens nach Beendigung des Auftrags.

Soweit der Auftragsverarbeiter eine nichtöffentliche Stelle ist, ist auch festzulegen, dass der Auftragsverarbeiter die Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu dulden hat. Diese Kontrolle richtet sich nach den maßgeblichen datenschutzrechtlichen Bestimmungen.

(4) Eine nichtöffentliche Stelle darf nur beauftragt werden, wenn

1. beim Verantwortlichen sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die übertragenen Aufgaben erheblich kostengünstiger erledigen kann und
2. die beim Auftragsverarbeiter mit der Datenverarbeitung beauftragten Beschäftigten besonders auf den Schutz der Personalaktendaten verpflichtet sind.

7. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
8. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
9. die Verpflichtung des Auftragnehmers, den Auftraggeber unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt und
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten, sobald diese für die Erfüllung des Auftrags nicht mehr benötigt werden, spätestens nach Beendigung des Auftrags.

Soweit der Auftragnehmer eine nichtöffentliche Stelle ist, ist auch festzulegen, dass der Auftragnehmer die Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu dulden hat. Diese Kontrolle richtet sich nach den maßgeblichen datenschutzrechtlichen Bestimmungen.

(4) Eine nichtöffentliche Stelle darf nur beauftragt werden, wenn

1. beim Auftraggeber sonst Störungen im Geschäftsablauf auftreten können oder der Auftragnehmer die übertragenen Aufgaben erheblich kostengünstiger erledigen kann und
2. die beim Auftragnehmer mit der Datenverarbeitung beauftragten Beschäftigten besonders auf den Schutz der Personalaktendaten verpflichtet sind.

Satz 1 Nummer 1 findet keine Anwendung für Gemeinden und Gemeindeverbände.

(5) Der Auftragsverarbeiter darf die Daten nur im Rahmen der Weisungen des Verantwortlichen verarbeiten. Der Auftragsverarbeiter darf die Daten nur für die im Auftrag festgelegten Zwecke verarbeiten und für die im Auftrag festgelegte Dauer speichern.

(6) Die Rechte der betroffenen Person nach dem geltenden Datenschutzrecht sind gegenüber dem Verantwortlichen geltend zu machen.

(7) Unteraufträge dürfen nur mit vorheriger Zustimmung des Verantwortlichen erteilt werden. Für Unterauftragsverarbeiter gelten die für den Auftragsverarbeiter bestehenden Vorgaben entsprechend.“

Artikel 8
Änderung des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz

Das Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz vom 17. Dezember 2015 (GV. NRW. S. 886) wird wie folgt geändert:

Satz 1 Nummer 1 findet keine Anwendung für Gemeinden und Gemeindeverbände.

(5) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer darf die Daten nur für die im Auftrag festgelegten Zwecke verarbeiten und nur für die im Auftrag festgelegte Dauer speichern.

(6) Die Rechte der betroffenen Person nach dem Datenschutzgesetz Nordrhein-Westfalen sind gegenüber dem Auftraggeber geltend zu machen.

(7) Unteraufträge dürfen nur mit vorheriger Zustimmung des Auftraggebers erteilt werden. Für Unterauftragnehmer gelten die für den Auftragnehmer bestehenden Vorgaben entsprechend.

Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz (BHKG)

§ 30
Externe Notfallpläne für schwere Unfälle mit gefährlichen Stoffen

(1) Für Betriebsbereiche im Sinne der Störfall-Verordnung in der Fassung der Bekanntmachung vom 8. Juni 2005 (BGBl. I S. 1598) in der jeweils geltenden Fassung, für die ein Sicherheitsbericht zu erstellen ist, haben die für den Katastrophenschutz zuständigen Kreise und kreisfreien Städte innerhalb von zwei Jahren nach Erhalt der erforderlichen Informationen von der Betreiberin oder vom Betreiber einen externen Notfallplan als Sonderschutzplan unter ihrer oder seiner Beteiligung und unter Berücksichtigung des internen Notfallplans (betrieblicher Alarm- und Gefahrenabwehrplan) zu erstellen, um

1. Schadensfälle einzudämmen und unter Kontrolle zu bringen, so dass die Auswirkungen möglichst gering gehalten und Schädigungen der menschlichen

Gesundheit, der Umwelt und von Sachwerten begrenzt werden können,
2. die erforderlichen Maßnahmen zum Schutz der menschlichen Gesundheit und der Umwelt vor den Auswirkungen schwerer Unfälle einzuleiten,
3. notwendige Informationen an die Öffentlichkeit sowie betroffene Behörden oder Dienststellen in dem betreffenden Gebiet weiterzugeben und
4. Aufräumarbeiten und Maßnahmen zur Wiederherstellung der Umwelt nach einem schweren Unfall einzuleiten.

Die zuständigen Kreise und kreisfreien Städte können aufgrund der Informationen in dem Sicherheitsbericht entscheiden, dass sich die Erstellung eines externen Notfallplans erübrigt; die Entscheidung ist zu begründen.

(2) Externe Notfallpläne müssen Angaben enthalten über

1. Namen oder Stellung der Personen, die zur Einleitung von Notfallmaßnahmen sowie zur Durchführung und Koordinierung von Maßnahmen außerhalb des Betriebsgeländes ermächtigt sind,
2. Vorkehrungen zur Entgegennahme von Frühwarnungen sowie zur Alarmauslösung und zur Benachrichtigung der Einsatzkräfte,
3. Vorkehrungen zur Koordinierung der zur Umsetzung des externen Notfallplans notwendigen Einsatzmittel,
4. Vorkehrungen zur Unterstützung von Abhilfemaßnahmen auf dem Betriebsgelände,
5. Vorkehrungen für Abhilfemaßnahmen außerhalb des Betriebsgeländes, einschließlich Reaktionsmaßnahmen auf Szenarien schwerer Unfälle, wie im Sicherheitsbericht beschrieben, unter Berücksichtigung möglicher Domino-Effekte, einschließlich solcher, die Auswirkungen auf die Umwelt haben,
6. Vorkehrungen zur Unterrichtung der Öffentlichkeit und aller benachbarten Betriebe oder Betriebsstätten, die nicht in den Anwendungsbereich der Störfall-Verordnung fallen, über den Unfall sowie über das richtige Verhalten und

7. Vorkehrungen zur Unterrichtung der Einsatzkräfte ausländischer Staaten bei einem schweren Unfall mit möglichen grenzüberschreitenden Folgen.

Die Betreiberin oder der Betreiber eines Betriebsbereichs hat dem zuständigen Kreis oder der zuständigen kreisfreien Stadt die für die Erstellung externer Notfallpläne erforderlichen Informationen unverzüglich, spätestens jedoch bis zum Ablauf eines Jahres nach dem Zeitpunkt, zu dem der Betriebsbereich dem Anwendungsbereich der Störfall-Verordnung unterfällt, zu übermitteln.

(3) Die Entwürfe der externen Notfallpläne sind zur Anhörung der Öffentlichkeit für die Dauer eines Monats öffentlich auszulegen. Die geheimhaltungsbedürftigen Teile der externen Notfallpläne, insbesondere dem Datenschutz unterliegende personenbezogene Angaben, verdeckte Telefonnummern oder interne Anweisungen, sind hiervon ausgenommen. Ort und Dauer der Auslegung sind vorher öffentlich bekanntzumachen mit dem Hinweis, dass Bedenken und Anregungen während der Auslegungsfrist vorgebracht werden können. Die fristgemäß vorgebrachten Bedenken und Anregungen sind zu prüfen; das Ergebnis ist mitzuteilen. Haben mehr als 50 Personen Bedenken und Anregungen mit im Wesentlichen gleichem Inhalt vorgebracht, kann die Mitteilung des Ergebnisses der Prüfung dadurch ersetzt werden, dass diesen Personen die Einsicht in das Ergebnis ermöglicht wird. Die Stelle, bei der das Ergebnis der Prüfung während der Dienststunden eingesehen werden kann, ist öffentlich bekanntzumachen. Wird der Entwurf des externen Notfallplans nach der Auslegung geändert oder ergänzt, ist er erneut auszulegen. Bei der erneuten Auslegung kann bestimmt werden, dass Bedenken oder Anregungen nur zu den geänderten oder ergänzten Teilen vorgebracht werden können. Werden durch die Änderung oder Ergänzung des Entwurfs die Grundzüge der Planung nicht berührt oder sind Änderungen oder Ergänzungen im Umfang geringfügig oder von geringer Bedeutung, kann von einer erneuten öffentlichen Auslegung abgesehen werden.

1. In § 30 Absatz 3 Satz 2 wird das Wort „Angaben“ durch das Wort „Daten“ ersetzt.

(4) Die Kreise und kreisfreien Städte haben die von ihnen erstellten externen Notfallpläne in angemessenen Abständen von höchstens drei Jahren unter Beteiligung der Betreiberin oder des Betreibers und unter Berücksichtigung des internen Notfallplans zu überprüfen, zu erproben und erforderlichenfalls zu überarbeiten und auf den neuesten Stand zu bringen. Bei dieser Überprüfung sind Veränderungen in den Betrieben und den Notdiensten, neue technische Erkenntnisse und Erkenntnisse darüber, wie bei schweren Unfällen zu handeln ist, zu berücksichtigen. Werden externe Notfallpläne nach der Überprüfung geändert oder aktualisiert, sind sie erneut gemäß Absatz 3 auszulegen.

2. § 46 wird wie folgt geändert:

a) In Absatz 1 werden nach dem Wort „Bestimmungen“ die Wörter „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) und“ eingefügt und die Wörter „in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542)“ werden durch die Angabe „vom [einsetzen: Ausfertigungsdatum und Fundstelle des neuen Datenschutzgesetzes]“ ersetzt.

§ 46
Verarbeitung personenbezogener Daten

(1) Für die Verarbeitung personenbezogener Daten gelten die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542) in der jeweils geltenden Fassung nach Maßgabe der folgenden Absätze.

b) Dem Absatz 2 wird folgender Satz angefügt:

„Die Verarbeitung personenbezogener Daten nach § 28 und § 38 ist nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 auch für besondere Kategorien gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 in Verbindung mit § 16 Nummer 1 des Datenschutzgesetzes Nordrhein-Westfalen zulässig.“

(2) Zur Vorbereitung und Durchführung vorbeugender und abwehrender Maßnahmen gegen Gefahren im Sinne des § 1 Absatz 1 dürfen die mit der Wahrnehmung dieser Aufgaben betrauten Behörden der Aufgabenträger und die hierbei mitwirkenden Organisationen und Einrichtungen personenbezogene Daten verarbeiten. Dies gilt insbesondere für Leitstellen und Auskunftsstellen nach Maßgabe der § 28 und § 38.

c) Absatz 3 wird wie folgt gefasst:

„(3) Die Informationspflicht des Verantwortlichen bei der Erhebung von personenbezogenen Daten bei der betroffenen Person nach Artikel 13 der Verordnung (EU) 2016/679 wird beschränkt. Gleiches gilt für die Informationspflicht des Verantwortlichen nach Artikel 14 der Verordnung (EU) 2016/679, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden.“

(3) Personenbezogene Daten sind grundsätzlich bei der betroffenen Person mit deren Kenntnis zu erheben. Bei Dritten dürfen personenbezogene Daten erhoben werden, soweit dies zum Schutz von Leben und Gesundheit, zur Sicherstellung einer wirksamen Gefahrenabwehr oder zur Geltendmachung von Kostenersatzansprüchen benötigten Angaben bei der betroffenen Person nicht oder nicht rechtzeitig erhoben werden können.

(4) Die nach § 28 Absatz 5 und § 38 Absatz 3 gespeicherten Daten dürfen in anonymisierter Form auch zu statistischen Zwecken und zur Evaluation verarbeitet sowie zur Aus- und Fortbildung genutzt werden. Die erhobenen Daten dürfen zu wissenschaftlichen Zwecken genutzt werden, wenn die darin enthaltenen personenbezogenen Daten vorher anonymisiert wurden. § 28 Datenschutzgesetz Nordrhein-Westfalen findet Anwendung.

d) Absatz 4 Satz 3 wird aufgehoben.

e) Absatz 5 wird aufgehoben.

(5) Auf der Grundlage dieses Gesetzes verarbeitete personenbezogene Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des Zwecks, zu dem sie erhoben wurden, nicht mehr erforderlich sind.

f) Absatz 6 wird Absatz 5.

(6) Die nach § 28 Absatz 5 gespeicherten, nicht anonymisierten Aufzeichnungen sind spätestens nach sechs Monaten zu löschen, es sei denn, dass sie zum Nachweis ordnungsgemäßer Ausführung der Aufgabe noch erforderlich sind oder Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange der oder des Betroffenen beeinträchtigt werden. Auf die Dokumentation des Funkverkehrs sowie die Datenerhebung in Auskunftsstellen nach § 38 Absatz 3 findet Satz 1 mit der Maßgabe Anwendung, dass die Daten des Funkverkehrs spätestens nach drei Monaten und die in Auskunftsstellen erhobenen Daten spätestens nach einem Monat zu löschen sind.

g) Absatz 7 wird Absatz 6 und wie folgt geändert:

aa) In Satz 1 wird die Angabe „6“ durch die Angabe „5“ ersetzt.
bb) Satz 2 wird aufgehoben.

(7) Nach Absatz 6 aufzubewahrende Daten sind zu sperren und mit einem Sperrvermerk zu versehen. Die §§ 8 und 10 des Datenschutzgesetzes Nordrhein-Westfalen finden Anwendung.

Artikel 9
Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen

Das Verfassungsschutzgesetz Nordrhein-Westfalen vom 20. Dezember 1994 (GV. NRW. 1995 S. 28), das zuletzt durch Gesetz vom [einsetzen: Ausfertigungsdatum und Fundstelle des Siebten Gesetzes zur Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen] geändert worden ist, wird wie folgt geändert:

1. Dem § 5 Absatz 1 wird folgender Satz angefügt:

„Die Verarbeitung ist auch zulässig, wenn der Betroffene eingewilligt hat.“

Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NRW -)

§ 5
Befugnisse

(1) Die Verfassungsschutzbehörde darf die zur Erfüllung ihrer Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten.

(2) Die Verfassungsschutzbehörde darf, soweit nicht der Schutz des Kernbereichs privater Lebensgestaltung entgegensteht, zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:

1. Einsatz von Vertrauenspersonen, sonstigen geheimen Informantinnen und Informanten, zum Zwecke der Spionageabwehr überworbenen Agentinnen und Agenten, Gewährspersonen und verdeckten Ermittlerinnen und Ermittlern unter den Voraussetzungen des § 7;
2. Observation, bei sicherheitsgefährdenden, geheimdienstlichen Tätigkeiten oder Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1, 3 und 4 von erheblicher Bedeutung auch mit besonderen, für Observationszwecke bestimmte technischen Mitteln; Observationen, die länger als einen Monat ununterbrochen andauern, bedürfen der Genehmigung durch die Leitung der Verfassungsschutzabteilung;
3. Bildaufzeichnungen (Fotografien, Videografieren und Filmen);
4. verdeckte Ermittlungen und Befragungen;
5. Mithören ohne Inanspruchnahme technischer Mittel;
6. Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes außerhalb von Wohnungen im Sinne des Artikels 13 des Grundgesetzes unter Einsatz technischer Mittel unter den Voraussetzungen des § 7a;
7. Beobachtung des Funkverkehrs auf nicht für den allgemeinen Empfang bestimmten Kanälen sowie die Sichtbarmachung, Beobachtung, Aufzeichnung und Entschlüsselung von Signalen in Kommunikationssystemen unter den Voraussetzungen des § 7a;
8. Verwendung fingierter biografischer, beruflicher oder gewerblicher Angaben (Legenden);
9. Beschaffung, Erstellung und Verwendung von Tarnpapieren und Tarnkennzeichen;
10. Abhören und Aufzeichnen der Telekommunikation und der Nutzung von Telemediendiensten sowie Öffnen und Einsehen der dem Brief- oder Postgeheimnis unterliegenden Sendungen unter den Voraussetzungen des § 7a;
11. Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte im Internet auf dem technisch hierfür für

jede Nutzerin und jeden Nutzer vorgesehenen Weg, ohne selbst Kommunikationsadressatin oder -adressat und ohne von den an der Kommunikation teilnehmenden Personen oder vergleichbaren Berechtigten hierzu autorisiert zu sein, unter den Voraussetzungen des § 7a; eine Online-Durchsuchung ist ausgeschlossen;

12. Einsatz technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes unter den Voraussetzungen des § 7b;
13. Erhebung von Auskünften über Beteiligte am Zahlungsverkehr und über Geldbewegungen und Geldanlagen bei Zahlungsdienstleistern unter den Voraussetzungen des § 7c Absatz 1;
14. Erhebung von Auskünften über Telekommunikationsverbindungsdaten und Nutzungsdaten von Telemediendiensten bei denjenigen, die geschäftsmäßig Telekommunikationsdienste und Telemediendienste erbringen oder daran mitwirken, unter den Voraussetzungen des § 7c Absatz 2;
15. Erhebung der nach den §§ 95 und 111 des Telekommunikationsgesetzes - das Inkrafttreten des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft in der Fassung der Bundesratsdrucksache 251/13, dem der Bundesrat am 3. Mai 2013 zugestimmt hat, ist jedoch abzuwarten - gespeicherten Daten bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes), auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokolladresse (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes), sowie Einholung von Auskünften nach § 14 Absatz 2 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, ohne dass die betroffene Person hierüber von den zur Auskunft Verpflichteten unterrichtet werden darf, unter den Voraussetzungen des § 7c Absatz 3.

(3) Die Verfassungsschutzbehörde darf zur Informationsbeschaffung nachrichtendienstliche Mittel nach Absatz 2 einsetzen, wenn Tatsachen die Annahme rechtfertigen, dass

1. auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 oder die zur Erlangung solcher Erkenntnisse erforderlichen Personen im Sinne des Absatzes 2 Nummer 1 gewonnen werden können oder
2. dies zum Schutz der Mitarbeiterinnen und Mitarbeiter, der Personen im Sinne des Absatzes 2 Nummer 1, der Einrichtungen und Gegenstände der Verfassungsschutzbehörde gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

(4) Sind für die Erfüllung der Aufgaben verschiedene Maßnahmen geeignet, hat die Verfassungsschutzbehörde diejenige auszuwählen, die die Betroffenen, insbesondere in ihren Grundrechten, voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann. Eine Maßnahme hat zu unterbleiben, wenn sie einen Nachteil herbeiführt, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

(5) Mit nachrichtendienstlichen Mitteln gewonnene personenbezogene Daten sind zu kennzeichnen und den Personen, zu denen diese Informationen erfasst wurden, nach Beendigung der Maßnahme mitzuteilen. Einer Mitteilung bedarf es nicht, wenn

1. eine Gefährdung der Aufgabenerfüllung durch die Benachrichtigung zu besorgen ist,
2. durch die Auskunftserteilung Personen nach Absatz 2 Nummer 1 gefährdet sein können oder die Offenlegung des Erkenntnisstandes oder der Arbeitsweise der Verfassungsschutzbehörde zu befürchten ist,
3. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem

Wohl des Bundes oder eines Landes Nachteile bereiten würde oder

4. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen

und eine der unter Nummer 1 bis 4 genannten Voraussetzungen auch fünf Jahre nach Beendigung der Maßnahme noch vorliegt und mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegen wird.

(6) Die mit nachrichtendienstlichen Mitteln erhobenen Daten dürfen an eine andere Stelle nur nach Maßgabe der §§ 17 bis 22 übermittelt werden, sofern sich aus § 5c Absatz 4 nichts anderes ergibt. Die Übermittlung ist zu dokumentieren.

(7) Die Verfassungsschutzbehörde darf Informationen, insbesondere Verfassungsschutzberichte, veröffentlichen. Dabei dürfen personenbezogene Daten nur veröffentlicht werden, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder die Darstellung von Organisationen erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse der betroffenen Person überwiegen.

(8) Die Befugnisse nach dem Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 5 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576) geändert worden ist, bleiben unberührt.

(9) Die Verfassungsschutzbehörde ist an die allgemeinen Rechtsvorschriften gebunden (Artikel 20 des Grundgesetzes). Polizeiliche Befugnisse oder Weisungsbefugnisse stehen der Verfassungsschutzbehörde nicht zu. Die Verfassungsschutzbehörde darf Polizeibehörden auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen sie selbst nicht befugt ist.

2. § 5c wird wie folgt geändert:

a) In Absatz 2 Satz 7 werden die Wörter „sind die Daten zu sperren und zu kennzeichnen“ durch die Wörter „ist die Verarbeitung der Daten einzuschränken“ ersetzt.

§ 5c
Übermittlungen, Löschungen und Mitteilungen bei Maßnahmen mit besonderer Eingriffsintensität

(1) Maßnahmen nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 sind unter Aufsicht einer oder eines von der Auswertung unabhängigen Bediensteten, die oder der die Befähigung zum Richteramt hat, vorzunehmen. Sie oder er entscheidet über die Übermittlung von auf diese Weise gewonnenen Daten und beaufsichtigt deren Löschung.

(2) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die mit nachrichtendienstlichen Mitteln nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 erhobenen personenbezogenen Daten allein oder zusammen mit bereits vorliegenden Daten für die Zwecke, zu denen sie erhoben wurden, erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung nach Absatz 5 oder für eine Überprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesen Fällen sind die Daten zu sperren und zu kennzeichnen; sie dürfen nur zu diesen Zwecken verwendet werden.

(3) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung gemäß Absatz 4 ist die Kennzeichnung durch den Empfänger aufrecht zu erhalten.

b) Absatz 4 wird wie folgt geändert:

aa) Dem Satz 1 wird folgender Satz vorangestellt:

„Die nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 erhobenen Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrags übermittelt werden.“

bb) Im neuen Satz 2 werden die Wörter „Die nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 erhobenen Daten dürfen“ durch die Wörter „An andere Stellen dürfen diese Daten“ ersetzt.

(4) Die nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 erhobenen Daten dürfen nur übermittelt werden

1. zur Verhinderung oder Aufklärung von Straftaten,

   a) wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 7a Absatz 1 Satz 1 Nummer 4 genannten Straftaten plant oder begeht oder
   b) bestimmte Tatsachen den Verdacht begründen, dass jemand

      aa) Straftaten nach den §§ 146, 151 bis 152a oder § 261 des Strafgesetzbuches in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 15. November 2012 (BGBl. I S. 2298) geändert worden ist,

bb) Straftaten nach § 34 Absatz 1 bis 6 und 8, § 35 des Außenwirtschaftsgesetzes in der Fassung der Bekanntmachung vom 27. Mai 2009 (BGBl. I S. 1150), das zuletzt durch Artikel 1 der Verordnung vom 12. Dezember 2012 (BAnz. 2012) geändert worden ist, §§ 19 bis 21 oder § 22a Absatz 1 Nummer. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506), das zuletzt durch Artikel 4 des Gesetzes vom 27. Juli 2011 (BGBl. I S. 1595) geändert worden ist,

cc) Straftaten nach § 29a Absatz 1 Nummer 2, § 30 Absatz 1 Nummer 1, 4 oder § 30a des Betäubungsmittelgesetzes in der Fassung der Bekanntmachung vom 1. März 1994 (BGBl. I S. 358), das zuletzt durch Artikel 4 des Gesetzes vom 19. Oktober 2012 (BGBl. I S. 2192) geändert worden ist,

dd) eine in § 129a des Strafgesetzbuches bezeichnete Straftat oder

ee) Straftaten nach den §§ 130, 232 Absatz 3, 4 oder Absatz 5 zweiter Halbsatz, §§ 249 bis 251, 255, 305a, 306 bis 306c, 307 Absatz 1 bis 3, § 308 Absatz 1 bis 4, § 309 Absatz 1 bis 5, §§ 313, 314, 315 Absatz 1, 3 oder Absatz 4, § 315b Absatz 3, §§ 316a, 316b Absatz 1 oder Absatz 3 oder § 316c Absatz 1 bis 3 des Strafgesetzbuches

plant oder begeht,

2. zur Verfolgung von Straftaten, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Nummer 1 bezeichnete Straftat begeht oder begangen hat, oder

cc) Nach Satz 2 wird der folgende Satz eingefügt:

„Die unter den Voraussetzungen des § 5 Absatz 5 Satz 2 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 2 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097) geändert worden ist, zulässige Übermittlung an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder schutzwürdige Interessen des Betroffenen entgegenstehen."

3. zur Vorbereitung und Durchführung eines Verfahrens nach Artikel 21 Absatz 2 Satz 2 des Grundgesetzes oder einer Maßnahme nach § 3 Absatz 1 Satz 1 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch Artikel 6 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) geändert worden ist,

soweit sie zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich sind. Die Übermittlung ist zu protokollieren. Sind mit personenbezogenen Daten weitere Daten der betroffenen Person oder Dritter in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung ist unzulässig. Absatz 2 gilt entsprechend. Die empfangende Stelle unterrichtet die übermittelnde Stelle unverzüglich über eine erfolgte Löschung.

(5) In den Fällen des § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 kann nach Beendigung der Maßnahme die Mitteilung an die betroffene Person nach § 5 Absatz 5 nur solange unterbleiben, wie eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. Erfolgt die Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Mitteilung der Zustimmung der G 10-Kommission. Die G 10-Kommission bestimmt die Dauer der weiteren Zurückstellung. Sobald das Mitteilungshindernis entfällt, ist die Mitteilung unverzüglich nachzuholen. Einer Mitteilung bedarf es nicht, wenn die G 10-Kommission einstimmig festgestellt hat, dass

1. diese Voraussetzung auch fünf Jahre nach Beendigung der Maßnahme noch nicht eingetreten ist und sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten wird und
2. die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch bei der empfangenden Stelle vorliegen.

Das für Inneres zuständige Ministerium unterrichtet alle drei Monate die G 10-Kommission über die von ihm vorgenommenen Mitteilungen an Betroffene oder über die Gründe, die einer Mitteilung entgegenstehen. Hält die G10-Kommission eine Mitteilung für geboten, so ist diese unverzüglich vorzunehmen. Wurden die Daten an eine andere Stelle übermittelt, erfolgt die Mitteilung im Benehmen mit der empfangenden Stelle.

3. § 10 wird wie folgt geändert:

a) In der Überschrift wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.

§ 10
Berichtigung, Löschung und Sperrung personenbezogener Daten in zur Person geführten Dateien

(1) Die Verfassungsschutzbehörde hat die in zur Person geführten Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit der in zur Person geführten Dateien gespeicherten personenbezogenen Daten von der betroffenen Person bestritten, ist dies in der Datei zu vermerken.

b) Absatz 2 Satz 4 wird wie folgt gefasst:

„In diesem Falle ist die Verarbeitung der Daten einzuschränken.“

(2) Die Verfassungsschutzbehörde hat die in zur Person geführten Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. § 4 des Archivgesetzes Nordrhein-Westfalen vom 16. März 2010 (GV. NRW. S. 188) bleibt unberührt. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß durch sie schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Falle sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung der betroffenen Person verarbeitet werden.

(3) Die Verfassungsschutzbehörde prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, ob gespeicherte Daten in zur Person geführten Dateien zu berichtigen oder zu löschen sind. In zur Person geführten Dateien gespeicherte personenbezogene Daten über Bestrebungen nach § 3 Abs. 1 Nr. 1 sind spätestens 10 Jahre, über Bestrebungen nach § 3 Abs. 1 Nr. 3 und 4 sind spätestens

15 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die Leitung der Verfassungsschutzabteilung stellt im Einzelfall fest, dass die weitere Speicherung zur Aufgabenerfüllung oder zur Wahrung schutzwürdiger Belange der betroffenen Person erforderlich ist. Die Gründe sind aktenkundig zu machen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

4. § 11 wird wie folgt geändert:

a) In der Überschrift wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.

§ 11
Berichtigung und Sperrung personenbezogener Daten in schriftlichen oder elektronischen Akten, Aktenvernichtung

(1) Stellt die Verfassungsschutzbehörde fest, daß in schriftlichen oder elektronischen Akten gespeicherte personenbezogene Daten unrichtig sind, sind sie zu berichtigen. Wird ihre Richtigkeit von der betroffenen Person bestritten, ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

b) Absatz 2 wird wie folgt gefasst:

„(2) Die Verfassungsschutzbehörde hat die Verarbeitung personenbezogener Daten in schriftlichen oder elektronischen Akten einzuschränken, wenn sie im Einzelfall feststellt, dass ohne die Einschränkung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden und die Daten für ihre künftige Aufgabenerfüllung nicht mehr erforderlich sind. Verarbeitungseingeschränkte Daten sind mit einem entsprechenden Vermerk zu versehen. Sie dürfen nur mit Einwilligung der betroffenen Person verarbeitet werden. Eine Aufhebung der Einschränkung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.“

(2) Die Verfassungsschutzbehörde hat personenbezogene Daten in schriftlichen oder elektronischen Akten zu sperren, wenn sie im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden und die Daten für ihre künftige Aufgabenerfüllung nicht mehr erforderlich sind. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nur noch mit Einwilligung der betroffenen Person verarbeitet werden. Eine Aufhebung der Sperrung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.

(3) Die Verfassungsschutzbehörde hat personenbezogene Daten in schriftlichen oder elektronischen Akten zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Sind personenbezogene Daten in schriftlichen oder elektronischen Akten gespeichert und ist eine Abtrennung nicht möglich, ist die Löschung nach Satz 1 Nummer 2 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist; es sei denn, dass die betroffene Person die Löschung verlangt und die weitere Speicherung sie in unangemessener Weise beeinträchtigen würde. Soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten auf Antrag der betroffenen Person zu sperren.

c) In Absatz 3 Satz 3 werden die Wörter „sind die“ durch die Wörter „ist die Verarbeitung der“ und die Wörter „zu sperren“ durch das Wort „einzuschränken“ ersetzt.

(4) Die Verfassungsschutzbehörde hat zur Person geführte Akten zu vernichten, wenn diese zu ihrer Aufgabenerfüllung nicht mehr erforderlich sind und der Vernichtung schutzwürdige Belange der betroffenen Person nicht entgegenstehen. Vor der Vernichtung ist die Freigabe durch die Leitung der Verfassungsschutzabteilung einzuholen. Für die Berichtigung und Sperrung von gespeicherten personenbezogenen Daten gelten die Absätze 1 und 2 entsprechend.

d) In Absatz 4 Satz 3 wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.

(5) § 4 des Archivgesetzes Nordrhein-Westfalen bleibt unberührt.

5. § 12 wird wie folgt gefasst:

„**§ 12**
Verfahrensverzeichnis

(1) Beim Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten führt die Verfassungsschutzbehörde ein für den behördlichen Datenschutzbeauftragten bestimmtes Verzeichnis.

§ 12
Verfahrensverzeichnis

(1) Beim Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten ist bei dem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis § 8 des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542), zuletzt geändert durch

(2) Das Verzeichnis enthält die folgenden Angaben:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. Angaben über den Kreis der betroffenen Personen,
4. Angaben über die Rechtsgrundlage der Verarbeitung,
5. eine Beschreibung der Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. gegebenenfalls die Verwendung von Profiling,
8. gegebenenfalls die beabsichtigte Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
9. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der personenbezogenen Daten und
10. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung.“

6. Nach § 14 wird folgender § 15 eingefügt:

„**§ 15**
Unabhängige Datenschutzkontrolle

(1) Jedermann kann sich an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit (die oder der Landesbeauftragte) wenden, wenn er der Ansicht ist,

Artikel 1 des Gesetzes vom 11. Juli 2011 (GV. NRW. S. 338), zu beachten.

(2) Auszüge aus Textdateien dürfen nicht ohne die dazugehörenden erläuternden Unterlagen übermittelt werden.

bei der Verarbeitung seiner personenbezogenen Daten durch die Verfassungsschutzbehörde in seinen Rechten verletzt worden zu sein.

(2) Die oder der Landesbeauftragte kontrolliert bei der Verfassungsschutzbehörde die Einhaltung der Vorschriften über den Datenschutz. Sie oder er berät die Verfassungsschutzbehörde in Belangen des Datenschutzes. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten, es sei denn, die G 10-Kommission ersucht die Landesbeauftragte oder den Landesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Die Verfassungsschutzbehörde ist verpflichtet, die Landesbeauftragte oder den Landesbeauftragten und ihre oder seine schriftlich besonders Beauftragten bei der Aufgabenerfüllung zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen, sowie
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

Dies gilt nicht, soweit die Verfassungsschutzbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(4) Die Absätze 1 bis 3 gelten ohne Beschränkung auf die Erfüllung der Aufgaben nach § 3. Sie gelten entsprechend für die Verarbeitung personenbezogener Daten durch andere Stellen, wenn

diese der Erfüllung der Aufgaben von Verfassungsschutzbehörden nach § 3 dient.

(5) Stellt die oder der Landesbeauftragte bei Datenverarbeitungen der Verfassungsschutzbehörde Verstöße gegen die Vorschriften über den Datenschutz fest, so beanstandet sie oder er dies gegenüber der Verfassungsschutzbehörde und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. Die oder der Landesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder zwischenzeitlich beseitigte Mängel handelt. Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Landesbeauftragten getroffen worden sind. Die oder der Landesbeauftragte kann die oder den Verantwortlichen davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen."

7. § 17 wird wie folgt geändert:

§ 17
Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörde

(1) Die Verfassungsschutzbehörde darf personenbezogene Daten an den Landtag und die Landesregierung übermitteln, wenn dies im Rahmen ihrer Aufgaben nach § 3 Absatz 2 erforderlich ist.

(2) Die Verfassungsschutzbehörde darf personenbezogene Daten, die mit den Mitteln nach § 5 Absatz 2 erhoben worden sind, an die Staatsanwaltschaften, die Finanzbehörden nach § 386 Absatz 1 der Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 5 des Gesetzes vom 3. Dezember 2015 (BGBl. I S. 2178) geändert worden ist, die Polizeien, die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden, die

Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen, übermitteln, soweit dies erforderlich ist zur

1. Erfüllung eigener Aufgaben der Informationsgewinnung (§ 5 Absatz 1),
2. Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,
3. Verhinderung oder sonstigen Verhütung von Straftaten von erheblicher Bedeutung im Sinne von § 7 Absatz 5 oder
4. Verfolgung von Straftaten von erheblicher Bedeutung im Sinne von § 7 Absatz 5.

§ 18 bleibt unberührt. Im Übrigen darf die Verfassungsschutzbehörde personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist oder die empfangende Stelle zum Zwecke der Erfüllung ihrer Aufgaben die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für erhebliche Zwecke der öffentlichen Sicherheit benötigt. Die empfangende Stelle darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihr übermittelt wurden.

(3) Die Verfassungsschutzbehörde darf personenbezogene Daten an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit die Bundesrepublik Deutschland dazu im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. II 1961 S. 1183, 1218) verpflichtet ist.

a) In Absatz 4 Satz 3 wird das Wort „Nutzungs-“ durch das Wort „Verwendungs-“ ersetzt.

(4) Die Verfassungsschutzbehörde darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben oder zur Abwehr einer erheblichen Gefahr für die empfangende Stelle erforderlich ist. Die Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen. Die Übermittlung unterbleibt ebenfalls, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines deutschen Gesetzes im Geltungsbereich des Grundgesetzes, insbesondere gegen die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Löschungsverpflichtung verstoßen wird. Die Übermittlung der von einer Ausländerbehörde empfangenen Daten unterbleibt, es sei denn, die Übermittlung ist völkerrechtlich geboten. Die Übermittlung ist aktenkundig zu machen. Die empfangende Stelle ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihr übermittelt wurden und daß die Verfassungsschutzbehörde sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

b) In Absatz 5 Satz 1 wird die Angabe „Absatz 2“ durch die Angabe „Absatz 4“ ersetzt.

(5) Personenbezogene Daten dürfen an andere Stellen nicht übermittelt werden, es sei denn, daß dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder der in § 3 Absatz 2 Nummer 2 genannten Einrichtungen erforderlich ist und die oder der für Inneres zuständige Ministerin oder Minister oder von ihr oder ihm besonders bestellte Beauftragte ihre Zustimmung erteilt haben. Die Verfassungsschutzbehörde führt über die Auskunft nach Satz 1 einen Nachweis, aus dem der Zweck der Übermittlung, ihre Veranlassung, die Aktenfundstelle und die empfangende Stelle hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Die empfangende Stelle darf die übermittelten Daten nur für den Zweck

verwenden, zu dem sie ihr übermittelt wurden. Die empfangende Stelle ist auf die Verwendungsbeschränkung und darauf hinzuweisen, daß die Verfassungsschutzbehörde sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten. Die Übermittlung der personenbezogenen Daten ist der betroffenen Person durch die Verfassungsschutzbehörde mitzuteilen, sobald eine Gefährdung ihrer Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist. Die Zustimmung der oder des für Inneres zuständigen Ministerin oder Ministers sowie das Führen eines Nachweises nach Satz 2 ist nicht erforderlich, wenn personenbezogene Daten durch die Verfassungsschutzbehörde zum Zweck von Datenerhebungen an andere Stellen übermittelt werden.

§ 21
Pflichten der empfangenden Stelle

Die empfangende Stelle prüft, ob die nach den Vorschriften dieses Gesetzes übermittelten personenbezogenen Daten für die Erfüllung ihrer Aufgaben erforderlich sind. Ergibt die Prüfung, daß sie nicht erforderlich sind, hat sie die Unterlagen zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand möglich ist; in diesem Fall sind die Daten zu sperren.

8. In § 21 Satz 3 werden die Wörter „sind die Daten zu sperren“ durch die Wörter „ist die Verarbeitung der Daten einzuschränken“ ersetzt.

§ 30
G 10-Kommission

(1) Zur Kontrolle der Maßnahmen der Verfassungsschutzbehörde nach § 5 Absatz 2 Nummer 6, 7 und 10 bis 14 in Verbindung mit §§ 7a bis 7c bestellt das Kontrollgremium nach Anhörung der Landesregierung für die Dauer der Wahlperiode des Landtags eine Kommission. Die G 10-Kommission besteht aus der oder dem Vorsitzenden, die oder der die Befähigung zum Richteramt besitzen muss, und vier Beisitzerinnen oder Beisitzern sowie fünf stellvertretenden Mitgliedern, die an den Sitzungen mit Rede- und Fragerecht teilnehmen können. Die Mitglieder der G 10-Kommission sind in ihrer Amtsführung

unabhängig und Weisungen nicht unterworfen. Sie nehmen ein öffentliches Ehrenamt wahr und werden von dem Kontrollgremium unverzüglich nach Anhörung der Landesregierung für die Dauer der Wahlperiode des Landtags mit der Maßgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der G 10-Kommission nach Ablauf der Wahlperiode endet. Das Kontrollgremium bestellt aus den Mitgliedern der G 10-Kommission die Vorsitzende oder den Vorsitzenden und seine Stellvertretung. Die G 10-Kommission tagt in Abständen von höchstens drei Monaten.

(2) Die Sitzungen der G 10-Kommmission sind geheim. Ihre Mitglieder sind zur Geheimhaltung aller Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit in der Kommission bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus der Kommission.

(3) Der G 10-Kommission ist die für ihre Aufgabenerfüllung notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags gesondert auszuweisen. Der Kommission sind bei Bedarf Mitarbeiterinnen oder Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen. § 27 Absatz 1 Satz 2 gilt entsprechend.

(4) Die G 10-Kommission gibt sich eine Geschäftsordnung, die der Zustimmung des Kontrollgremiums bedarf. Vor der Zustimmung ist die Landesregierung zu hören.

9. § 30 Absatz 5 wird wie folgt geändert:

a) In Satz 2 werden die Wörter „Erhebung, Verarbeitung und Nutzung“ durch das Wort „Verarbeitung“ ersetzt.

(5) Die G 10-Kommission entscheidet von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen. Die Kontrollbefugnis der G 10-Kommission erstreckt sich auf die Erhebung, Verarbeitung und Nutzung der durch die Beschränkungsmaßnahmen erlangten personenbezogenen Daten einschließlich der Entscheidung über die Mitteilung an Betroffene. Der G 10-Kommission und ihren Mitarbeiterinnen oder Mitarbeitern ist dabei insbesondere

1. Auskunft zu ihren Fragen zu erteilen,
2. Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Beschränkungsmaßnahme stehen, und
3. jederzeit Zutritt in alle Diensträume zu gewähren.

Die G 10-Kommission kann der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben. Auf § 24 Absatz 2 Satz 3 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel I des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist, wird verwiesen.

b) Satz 5 wird wie folgt gefasst:

„Auf § 15 Absatz 2 Satz 2 wird hingewiesen.“

(6) Beschlüsse der G 10-Kommission bedürfen der Mehrheit der Stimmen der anwesenden Mitglieder. Für Entscheidungen über die endgültige Nichtmitteilung gilt § 5c Absatz 5 Satz 5. Bei Stimmengleichheit entscheidet die Stimme der oder des Vorsitzenden. Die Kommission unterrichtet das Kontrollgremium über die von ihr gefassten Beschlüsse.

(7) Die G 10-Kommission darf ihr zur Erfüllung ihrer Aufgaben durch die Verfassungsschutzbehörde übermittelte personenbezogene Daten speichern. Sofern die übermittelten Daten für die Aufgabenerfüllung nicht mehr erforderlich sind, sind sie zu löschen.

(8) Die Mitglieder der G 10-Kommission erhalten eine Aufwandsentschädigung, Sitzungstagegelder und Ersatz der Reisekosten nach Maßgabe einer von der Landesregierung zu erlassenden Rechtsverordnung.

10. § 31 wird wie folgt gefasst:

„§ 31
Ausschluss der Anwendbarkeit des Datenschutzgesetzes Nordrhein-Westfalen und Anwendung des Bundesdatenschutzgesetzes

(1) Bei der Aufgabenerfüllung durch die Verfassungsschutzbehörde findet das Datenschutzgesetz Nordrhein-Westfalen vom [einsetzen: Ausfertigungsdatum und Fundstelle] keine Anwendung.

(2) Die §§ 2, 3, 5 Absatz 1 bis 3 und 5, §§ 6, 7, 42, 46, 51 Absatz 1 bis 4, §§ 52 bis 54, 62, 64 bis 66, 83 und 84 des Bundesdatenschutzgesetzes sind entsprechend anzuwenden, soweit nicht in diesem Gesetz abweichende Regelungen enthalten sind. Wird in den genannten Vorschriften auf europarechtliche Regelungen Bezug genommen, führt dies nicht zu einer Anwendbarkeit der europarechtlichen Regelungen.“

§ 31
Geltung des Datenschutzgesetzes Nordrhein-Westfalen

Bei der Erfüllung der Aufgaben durch die Verfassungsschutzbehörde finden die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen Anwendung; es sei denn zu demselben Sachverhalt werden in diesem Gesetz besondere Regelungen getroffen.

Artikel 10
Änderung des Sicherheitsüberprüfungsgesetzes Nordrhein-Westfalen

Das Sicherheitsüberprüfungsgesetz Nordrhein-Westfalen vom 7. März 1995 (GV. NRW. S. 210), das zuletzt durch Artikel 9 des Gesetzes vom 5. April 2005 (GV. NRW. S. 306) geändert worden ist, wird wie folgt geändert:

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Nordrhein-Westfalen (Sicherheitsüberprüfungsgesetz Nordrhein-Westfalen - SÜG NW -)

1. § 21 wird wie folgt geändert:

   a) In der Überschrift wird das Wort „Nutzen“ durch das Wort „Verwenden“ ersetzt.

§ 21
Speichern, Verändern und Nutzen personenbezogener Daten in Dateien

(1) Die zuständige Stelle darf zur Erfüllung ihrer Aufgaben nach diesem Gesetz

1. die in § 14 Abs. 1 Nr. 1 und 2 genannten personenbezogenen Daten der betroffenen Person, ihre Aktenfundstelle und die der mitwirkenden Behörde,
2. die Bezeichnung der Beschäftigungsstelle,

3. Verfügungen zur Bearbeitung des Vorganges sowie
4. die Bezeichnung der beteiligten Behörden

b) In Absatz 1 wird im Textteil nach Nummer 4 das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.

in Dateien speichern, verändern und nutzen.

(2) Die mitwirkende Behörde darf zur Erfüllung ihrer Aufgaben

1. die in § 14 Abs. 1 Nr. 1 bis 6 genannten personenbezogenen Daten der betroffenen Person und der in die Sicherheitsüberprüfung einbezogenen Person und die Aktenfundstelle,
2. Verfügungen zur Bearbeitung des Vorgangs sowie
3. sicherheitserhebliche Erkenntnisse und Erkenntnisse, die ein Sicherheitsrisiko begründen,

c) In Absatz 2 Satz 1 wird im Textteil nach Nummer 3 das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.

in Dateien speichern, verändern und nutzen. Die Daten nach Nummer 1 dürfen auch in den nach § 6 des Bundesverfassungsschutzgesetzes zulässigen Verbunddateien gespeichert werden.

2. § 22 wird wie folgt geändert:

§ 22
Übermittlung und Zweckbindung

a) Absatz 1 wird wie folgt geändert:

(1) Die im Rahmen der Sicherheitsüberprüfung gespeicherten personenbezogenen Daten dürfen von der zuständigen Stelle oder mitwirkenden Behörde nur für

1. die mit der Sicherheitsüberprüfung verfolgten Zwecke,
2. Zwecke der Verfolgung von Straftaten von erheblicher Bedeutung (§ 8 Abs. 3 PolG NW),
3. Zwecke parlamentarischer Untersuchungsausschüsse

aa) In Satz 1 wird das Wort „genutzt“ durch das Wort „verwendet“ ersetzt.

genutzt und übermittelt werden.

Die Strafverfolgungsbehörden dürfen die ihnen nach Satz 1 Nr. 2 übermittelten Daten für Zwecke eines Strafverfahrens nur verwenden, wenn die Strafverfolgung auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die

	zuständige Stelle darf die gespeicherten personenbezogenen Daten darüber hinaus für Zwecke der disziplinarrechtlichen Verfolgung sowie dienst- oder arbeitsrechtlicher Maßnahmen nutzen und übermitteln, wenn dies zur Gewährleistung des Verschlußsachenschutzes erforderlich ist. Die mitwirkende Behörde darf die gespeicherten personenbezogenen Daten darüber hinaus im Rahmen des erforderlichen Umfangs nutzen und übermitteln zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten oder zur Aufklärung sonstiger Bestrebungen von erheblicher Bedeutung.
bb) In Satz 3 und 4 wird jeweils das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.	
	(2) Die Übermittlung der nach § 21 in Dateien gespeicherten Daten ist nur zulässig, soweit sie für die Erfüllung der in Absatz 1 genannten Zwecke erforderlich ist. Die nach § 21 Abs. 2 Nr. 1 gespeicherten Daten dürfen zur Erfüllung aller Zwecke des Verfassungsschutzes genutzt und übermittelt werden.
b) In Absatz 2 Satz 2 wird das Wort „genutzt“ durch das Wort „verwendet“ ersetzt.	
	(3) Die mitwirkende Behörde darf personenbezogene Daten nach den Absätzen 1 und 2 nur an öffentliche Stellen übermitteln.
	(4) Die Nutzung oder Übermittlung unterbleibt, soweit gesetzliche Verwendungsregelungen entgegenstehen.
c) In Absatz 5 werden die Wörter „und nutzen“ gestrichen.	(5) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten und nutzen, zu dessen Erfüllung sie ihm übermittelt werden.

3. § 23 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

„**§ 23** **Berichtigung, Löschung und Verarbeitungseinschränkung personenbezogener Daten**“	**§ 23** **Berichtigen, Löschen und Sperren personenbezogener Daten**

(1) Die zuständige Stelle und die mitwirkende Behörde haben personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit personenbezogener Daten von der betroffenen Person bestritten, so ist dies, soweit sich die personenbezogenen Daten in Akten befinden, dort zu vermerken, bei Dateien auf sonstige Weise festzuhalten. Zuständige Stelle und mitwirkende Behörde haben sich jeweils gegenseitig zu unterrichten.

(2) In Dateien gespeicherte personenbezogene Daten sind zu löschen

1. von der zuständigen Stelle
   a) innerhalb eines Jahres nach Abschluß der Sicherheitsüberprüfung, wenn die betroffene Person keine sicherheitsempfindliche Tätigkeit aufnimmt, es sei denn, die betroffene Person willigt in die weitere Speicherung ein,
   b) nach Ablauf von fünf Jahren nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit, es sei denn, die betroffene Person willigt in die weitere Speicherung ein oder es ist beabsichtigt, die betroffene Person in absehbarer Zeit mit einer sicherheitsempfindlichen Tätigkeit zu betrauen;
2. von der mitwirkenden Behörde
   a) bei einfachen Sicherheitsüberprüfungen nach Ablauf von fünf Jahren nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit,
   b) bei den übrigen Überprüfungsarten nach Ablauf von zehn Jahren nach den in Ziffer 1 genannten Fristen,

c) die nach § 21 Abs. 2 Nr. 3 gespeicherten Daten, wenn feststeht, daß die betroffene Person keine sicherheitsempfindliche Tätigkeit aufnimmt oder aus ihr ausgeschieden ist.

Im übrigen sind in Dateien gespeicherte personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist.

b) Absatz 3 wird wie folgt geändert:

aa) In Satz 2 werden die Wörter „sind die Daten zu sperren“ durch die Wörter „ist die Verarbeitung der Daten einzuschränken“ ersetzt.

bb) In Satz 3 werden die Wörter „und genutzt“ gestrichen.

(3) Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß durch sie schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Fall sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung der betroffenen Person verarbeitet und genutzt werden.

4. § 28 wird wie folgt geändert:

§ 28
Abschluß der Sicherheitsüberprüfung, Weitergabe sicherheitserheblicher Erkenntnisse

a) In Satz 1 wird das Wort „nicht-öffentliche“ durch das Wort „nichtöffentliche“ ersetzt.

Die zuständige Stelle unterrichtet die nichtöffentliche Stelle nur darüber, daß die betroffene Person mit einer sicherheitsempfindlichen Tätigkeit betraut oder nicht betraut werden kann. Erkenntnisse, die die Ablehnung der Betrauung mit einer sicherheitsempfindlichen Tätigkeit betreffen, dürfen nicht mitgeteilt werden. Zur Gewährleistung des Geheim- und Sabotageschutzes können sicherheitserhebliche Erkenntnisse an die nicht-öffentliche Stelle übermittelt werden und dürfen von ihr ausschließlich zu diesem Zweck genutzt werden. Die nicht-öffentliche Stelle hat die zuständige Stelle unverzüglich zu unterrichten, wenn sicherheitserhebliche Erkenntnisse über die betroffene Person oder die in die Sicherheitsüberprüfung einbezogene Person bekannt werden.

b) In Satz 3 werden das Wort „nicht-öffentliche“ durch das Wort „nichtöffentliche“ und das Wort „genutzt“ durch das Wort „verwendet“ ersetzt.

c) In Satz 4 wird das Wort „nicht-öffentliche“ durch das Wort „nichtöffentliche“ ersetzt.

5. § 32 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

„**§ 32** **Datenverarbeitung in Dateien nichtöffentlicher Stellen**“	**§ 32** **Datenverarbeitung, -nutzung und -berichtigung in Dateien**
b) In Satz 1 werden die Wörter „nichtöffentliche“ durch das Wort „nichtöffentliche“ und das Wort „nutzen“ durch das Wort „verwenden“ ersetzt. c) In Satz 2 wird das Wort „Sperrung“ durch das Wort „Verarbeitungseinschränkung“ ersetzt.	Die nicht-öffentliche Stelle darf die nach diesem Gesetz zur Erfüllung ihrer Aufgaben erforderlichen personenbezogenen Daten der betroffenen Person in Dateien speichern, verändern und nutzen. Die für die zuständige Stelle geltenden Vorschriften zur Berichtigung, Löschung und Sperrung finden Anwendung.
6. § 34 wird wie folgt geändert:	**§ 34** **Allgemeine Verwaltungsvorschriften**
	Die allgemeinen Verwaltungsvorschriften erläßt
a) In Nummer 1 wird das Wort „Innenministerium“ durch die Wörter „für Inneres zuständige Ministerium“ ersetzt.	1. zur Ausführung des Ersten Teils dieses Gesetzes und des § 33 das Innenministerium,
b) In Nummer 2 werden die Wörter „Ministerium für Wirtschaft, Mittelstand und Technologie“ durch die Wörter „für Wirtschaft zuständige Ministerium“ und das Wort „Innenministerium“ durch die Wörter „für Inneres zuständigen Ministerium“ ersetzt.	2. zur Ausführung des Zweiten Teils dieses Gesetzes das Ministerium für Wirtschaft, Mittelstand und Technologie im Einvernehmen mit dem Innenministerium.
7. Nach § 34 werden die folgenden §§ 34a bis 34d eingefügt:	
„**§ 34a** **Anwendung bundesrechtlicher Vorschriften bei der Datenverarbeitung durch öffentliche Stellen**	
(1) Bei der Erfüllung der Aufgaben dieses Gesetzes durch öffentliche Stellen findet das Datenschutzgesetz Nordrhein-Westfalen vom [einsetzen: Ausfertigungsdatum und Fundstelle] keine Anwendung.	

(2) Die §§ 2, 3, 5 Absatz 1 bis 3 und 5, §§ 6, 7, 42, 46, 51 Absatz 1 und 3, §§ 52, 53, 54 Absatz 1 und 2 sowie §§ 62, 64 bis 66 und 83 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) sind entsprechend anzuwenden, soweit nicht in diesem Gesetz abweichende Regelungen enthalten sind. Wird in den genannten Vorschriften auf europarechtliche Regelungen Bezug genommen, führt dies nicht zu einer Anwendbarkeit der europarechtlichen Regelungen.

§ 34b
Anwendung bundesrechtlicher Vorschriften bei der Datenverarbeitung durch nichtöffentliche Stellen

(1) Bei der Erfüllung der Aufgaben dieses Gesetzes durch nichtöffentliche Stellen finden § 1 Absatz 8, §§ 16 bis 21 sowie § 85 des Bundesdatenschutzgesetzes keine Anwendung.

(2) Die §§ 42, 46, 51 Absatz 1 und 3, §§ 52, 53, 54 Absatz 1 und 2 und §§ 62, 64 bis 66 und 83 des Bundesdatenschutzgesetzes sind entsprechend anzuwenden, soweit nicht in diesem Gesetz abweichende Regelungen enthalten sind.

§ 34c
Unabhängige Datenschutzkontrolle

(1) Jedermann kann sich an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit (die oder der Landesbeauftragte) wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten nach diesem Gesetz durch öffentliche oder nichtöffentliche Stellen in seinen Rechten verletzt worden zu sein.

(2) Die oder der Landesbeauftragte kontrolliert bei den öffentlichen und nichtöffentlichen Stellen die Einhaltung der Vorschriften über den Datenschutz. Sie

oder er berät die öffentlichen und nichtöffentlichen Stellen in Belangen des Datenschutzes. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten, es sei denn, die G 10-Kommission ersucht die Landesbeauftragte oder den Landesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) Die öffentlichen und nichtöffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten und ihre oder seine schriftlich besonders beauftragten Personen bei der Aufgabenerfüllung zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen, sowie
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

Dies gilt nicht, soweit die zuständige oberste Landesbehörde oder die oberste Aufsichtsbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(4) Stellt die oder der Landesbeauftragte bei Datenverarbeitungen der öffentlichen oder nichtöffentlichen Stellen Verstöße gegen die Vorschriften über den Datenschutz fest, beanstandet sie oder er dies gegenüber der obersten Landesbehörde oder der obersten Aufsichtsbehörde und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. Die oder der Landesbeauftragte kann von einer Beanstandung absehen oder

auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder zwischenzeitlich beseitigte Mängel handelt. Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Landesbeauftragten getroffen worden sind. Die oder der Landesbeauftragte kann den Verantwortlichen davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

§ 34d
Verfahrensverzeichnis

(1) Beim Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten führt die öffentliche Stelle ein für den behördlichen Datenschutzbeauftragten bestimmtes Verzeichnis.

(2) Das Verzeichnis enthält die folgenden Angaben:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsamen mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. Angaben über den Kreis der betroffenen Personen,
4. Angaben über die Rechtsgrundlage der Verarbeitung,
5. eine Beschreibung der Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. gegebenenfalls die Verwendung von Profiling,

8. gegebenenfalls die beabsichtigte Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
9. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der personenbezogenen Daten und
10. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 64 des Bundesdatenschutzgesetzes.“

Artikel 11
Inkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

Begründung

Begründung zu Artikel 1 Datenschutzgesetz Nordrhein-Westfalen

Allgemein

Am 25. Mai 2016 ist die 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. Mai 2016, S. 1 ff.) (DSGVO) in Kraft getreten. Gemäß Artikel 99 Absatz 2 DSGVO gilt sie ab dem 25. Mai 2018.

Nach Artikel 288 des Vertrages über die Arbeitsweise der Europäischen Union gelten EU-Verordnungen unmittelbar und bedürfen keiner Umsetzung in das mitgliedstaatliche Recht. Ungeachtet dessen enthält die DSGVO zum einen Öffnungsklauseln für den nationalen Gesetzgeber und zum anderen konkrete Regelungsaufträge. Der sich daraus ergebende Anpassungsbedarf des Landesrechts in Nordrhein-Westfalen soll mit diesem Gesetz umgesetzt werden.

Gleichzeitig dient dieses Gesetz auch 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 Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89 ff.) (DS-RL), soweit die Mitgliedstaaten nach Artikel 63 der Richtlinie verpflichtet sind, Rechts- und Verwaltungsvorschriften zu erlassen, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016/680 wird darüber hinaus gesondert im Fachrecht erfolgen.

Ziel des Gesetzentwurfs ist es, wie bisher im Bereich des allgemeinen Datenschutzes einen einheitlichen Rechtsrahmen zu schaffen, der von allen öffentlichen Stellen gleichermaßen zu beachten ist. Dies hat vor allem Vorteile im Bereich des technischen und organisatorischen Datenschutzes, der Datenschutzkontrolle und für besondere Datenverarbeitungen, die grundsätzlich in allen öffentlichen Stellen zur Anwendung kommen können, wie z.B. die Personaldatenverarbeitung oder die Datenverarbeitung für wissenschaftliche und historische Forschungszwecke.

Ziel des Gesetzentwurfs ist es außerdem, den bisherigen Datenschutzstandard des Landes Nordrhein-Westfalen zu erhalten, insbesondere was die materiellen Anforderungen an die Datenverarbeitung anbelangt. Mit der Neufassung soll der Systemwechsel im Datenschutzrecht mit dem Vorrang der DSGVO und lediglich ergänzender Anwendung des Landesrechts deutlich gemacht werden.

Die Nachhaltigkeitspostulate werden vom vorliegenden Gesetzentwurf nicht berührt. Konflikte mit der Nachhaltigkeitsstrategie NRW bestehen nicht.

Im Besonderen: zu den einzelnen Vorschriften

Teil 1 Aufgabe dieses Gesetzes

Begründung zu § 1 Zweck

Zu Absatz 1

Das Gesetz dient dazu, die für die Durchführung der DSGVO notwendigen ergänzenden Regelungen zu treffen und gleichzeitig spezifische Anforderungen an die Verarbeitung personenbezogener Daten zu definieren (Teil 2 dieses Gesetzes). Für die Anwender und die betroffenen Personen soll durch die vorangestellte Stellung der Norm deutlich werden, dass dieses Gesetz die DSGVO lediglich ergänzt. Dies bedeutet für die Praxis, dass zunächst die DSGVO anzuwenden ist und das DSG NRW bzw. spezielle Vorschriften diese ergänzen. Dies gilt insbesondere dort, wo Handlungsaufträge der DSGVO erfüllt und Handlungsoptionen wahrgenommen worden sind.

Zu Absatz 2

Die Richtlinie (EU) 2016/680 (DS-RL) ist in Landesrecht umzusetzen. Zur Vereinheitlichung des Datenschutzniveaus soll der von der DSGVO gesteckte Rechtsrahmen, soweit möglich, auch auf Datenverarbeitungen erstreckt werden, die dem Anwendungsbereich der DS-RL unterfallen. Dies geschieht im Wesentlichen durch Verweisungen auf die DSGVO und Teil 2 dieses Gesetzes. Wo dies nicht möglich ist, sind eigenständige Regelungen für den Anwendungsbereich der DS-RL getroffen worden. Insofern dient das DSG NRW auch der Umsetzung der DS-RL (Teil 3 dieses Gesetzes). Soweit wegen der besonderen Sachmaterie der DS-RL abweichende Sonderregelungen für einzelne Anwendergruppen zu treffen sind, werden diese im Fachrecht geregelt.

Begründung zu § 2 Sicherstellung des Datenschutzes

§ 2 greift das Prinzip der eigenverantwortlichen Durchführung des Datenschutzes im jeweiligen Verantwortungsbereich auf, wie es bisher in § 7 DSG a. F. geregelt war. Dieses Prinzip steht auch nicht in Widerspruch mit der Datenschutz-Grundverordnung oder der Richtlinie (EU) 2016/680. Es steht vielmehr im Einklang mit den gesetzlichen Zuständigkeiten für die konkrete Datenverarbeitung bei einer öffentlichen Stelle (verantwortliche Stelle) und beachtet auch die Sonderstellung der unabhängigen Aufsichtsbehörde, wie sie in Artikel 39 Absatz 1 Buchstabe b) DSGVO geregelt ist. Die Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften im jeweiligen Geschäftsbereich ist Teil der aus dem Ressortprinzip abzuleitenden generellen Pflicht dieser Stellen, die Rechtmäßigkeit der ihnen unterstellten Verwaltung zu gewährleisten. Die Gemeinden und die Gemeindeverbände trifft diese (jeweilige) Verantwortung ebenfalls originär. Aufgrund der kommunalen Selbstverwaltungsgarantie nach Artikel 28 Absatz 2 Grundgesetz unterliegen sie zwar einer eingeschränkten Aufsicht (Rechtsaufsicht), sie gehören aber nicht zum Geschäftsbereich einer obersten Landesbehörde, wie es bei einer nachgeordneten Landesbehörde der Fall ist.

Die Verpflichtung zur Selbstkontrolle, wie sie in § 2 zum Ausdruck kommt, bleibt eine wichtige Maßnahme zur präventiven Sicherung des Datenschutzes.

§ 2 gilt für sämtliche Teile dieses Gesetzes.

Begründung zu § 3 Zulässigkeit der Verarbeitung personenbezogener Daten

Mit § 3 wird eine allgemeine Rechtsgrundlage für die Datenverarbeitung durch öffentliche Stellen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e i.V.m. Artikel 6 Absatz 3 Satz 1 Buchstabe b DSGVO und Artikel 8 DS-RL geschaffen. Da in der DSGVO und der DS-RL selbst nur ein Regelungsauftrag in Richtung nationaler Gesetzgebung formuliert ist, wird dieser Auftrag mit diesem Gesetz für das Land Nordrhein-Westfalen erfüllt.

Zu Absatz 1

Der Verarbeitungsbegriff folgt dabei unmittelbar aus Artikel 4 Nummer 2 DSGVO. Durch die „Verarbeitung durch öffentliche Stellen“ wird damit insbesondere auch jede Form der Bereitstellung (Übermittlung, Verbreitung etc.) personenbezogener Daten sämtlicher öffentlicher Stellen, also auch innerhalb einer öffentlichen Stelle umfasst. Hierdurch ist sichergestellt, dass innerhalb einer öffentlichen Stelle dem einzelnen Bediensteten nur die personenbezogenen Daten zur Kenntnis gelangen, die für die Aufgabenerledigung im Einzelnen auch benötigt werden (Grundsatz informationeller Gewaltenteilung). Sofern ausnahmsweise eine Differenzierung für die Übermittlung innerhalb einer öffentlichen Stelle gegenüber der Übermittlung zwischen verschiedenen öffentlichen Stellen gerechtfertigt erscheint, wird diese gesondert durch dieses Gesetz geregelt.

Die Regelung des Absatzes 1 umfasst dabei auch die Übermittlung personenbezogener Daten an öffentliche Stellen, wenn sie nur zur Erfüllung der in der Zuständigkeit der empfangenen Stelle liegenden Aufgaben erforderlich ist.

Welche Aufgaben in der Zuständigkeit des Verantwortlichen liegen und ihm insoweit im Sinne von Artikel 6 Absatz 1 Buchstabe e DSGVO die Ausübung öffentlicher Gewalt übertragen wurde, kann sich sowohl aus nationalen Rechtsvorschriften als auch aus europarechtlichen Vorgaben ergeben. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf der Grundlage der weiteren in Artikel 6 Absatz 1 DSGVO aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der DSGVO und der Richtlinie zum Datenschutz bei Polizei und Justiz erlassenen bereichsspezifischen Regelungen.

Zu Absatz 2

Die Regelung in Absatz 2 Satz 1 baut auf § 4 Absatz 6 DSG NRW a.F. auf. Die Regelung ist geboten, um der Problematik Rechnung zu tragen, dass bei der Verarbeitung personenbezogener Daten nicht immer eine Trennung nach erforderlichen und nicht erforderlichen Daten mit vertretbarem Aufwand möglich ist. Anders noch als es § 4 Absatz 6 DSG NRW a.F. vorsieht, bezieht sich die Vorschrift nicht bloß auf eine Verarbeitung in Akten. Die Problematik der Untrennbarkeit ist genauso in Konstellationen automatisierter Verfahren denkbar und wird daher auf jedwede Verarbeitungssituation ausgedehnt. Ist eine Trennung der Daten mit vertretbarem Aufwand (betrifft insbesondere Maßnahmen wie die Vervielfältigung bei Papierakten oder die Unkenntlichmachung der jeweiligen Daten) nicht möglich, dürfen ausnahmsweise auch nicht für konkrete Zwecke erforderliche Daten übermittelt werden. Eine Abwägung mit ggf. entgegenstehenden Belangen der betroffenen Personen hat zu erfolgen.
Satz 2 normiert ein Verwertungsverbot der nicht erforderlichen Daten zum Schutz der Rechte der betroffenen Personen. Die Regelungsbefugnis ergibt sich aus Artikel 6 Absätze 2 und 3 DSGVO.

Teil 2 Durchführungsbestimmungen zur Verordnung (EU) 2016/679

Kapitel 1 Allgemeine Bestimmungen

Begründung zu § 4 Begriffsbestimmung

Artikel 4 der Verordnung (EU) 2016/679 enthält eine Vielzahl von Begriffsdefinitionen. Unter anderem wird in Artikel 4 Ziffer 5 der Verordnung (EU) 2016/679 der Begriff des „Pseudonymisierens“ definiert. Bislang enthielt das DSG NRW a.F. neben der Definition dieses Begriffs auch eine Definition des Begriffs „Anonymisierung“. Bei der Anonymisierung personenbezogener Daten handelt es sich um einen Verarbeitungsvorgang, der in einigen bereichsspezifischen Rechtsvorschriften zum Schutz der Rechte und Freiheiten der betroffenen Personen und als Maßnahme zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung personenbezogener Daten normiert ist. Es ist daher erforderlich, diesen Begriff weiterhin im allgemeinen Recht zu definieren. Die Regelungsbefugnis ergibt sich aus Artikel 6 Absätze 2 und 3 der Verordnung (EU) 2016/679. Danach dürfen Mitgliedstaaten Regelungen einführen oder beibehalten, die spezifischen Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.

Begründung zu § 5 Anwendungsbereich

Zu den Absätzen 1 bis 4

Teil 2 dieses Gesetzes soll wie bisher das DSG NRW für alle öffentlichen Stellen des Landes Nordrhein-Westfalen ungeachtet ihrer Organisationsform, für die Gemeinden und Gemeindeverbände im Land Nordrhein-Westfalen sowie für die juristischen Personen des öffentlichen Rechts und Beliehene gelten, soweit diese personenbezogene Daten verarbeiten.

Ausnahmen gelten wie bisher für die Gerichte, die Staatsanwaltschaften, den Landesrechnungshof und die Staatlichen Rechnungsprüfungsämter sowie den Landtag, soweit diese Stellen keine Verwaltungsaufgaben wahrnehmen. Speziell für den Landtag wird darüber hinaus die Anwendbarkeit der DSGVO erklärt, da die Tätigkeit eines Parlaments eigentlich nicht Gegenstand des Unionsrechtes ist. Es bleibt dem Landtag unter Berücksichtigung seiner verfassungsrechtlichen Stellung überlassen, im Rahmen seiner Autonomie gegebenenfalls eine Datenschutzordnung zu erlassen.
Absatz 1 Satz 2 entspricht § 2 Absatz 2 Satz 3 DSG NRW a.F. und erfüllt eine klarstellende Funktion.
Die Datenverarbeitung der in Absatz 4 benannten Stellen zu wirtschaftlichen Zwecken unterliegt ebenfalls nicht den Regelungen für öffentliche Stellen. Für den Bereich der wirtschaftlichen Tätigkeit gelten die für nicht-öffentliche Stellen geltenden Regelungen der DSGVO und ergänzend dazu des Bundesdatenschutzgesetzes bzw. weiterer spezieller Gesetze. Die Chancengleichheit im Wettbewerb wird insoweit hergestellt.
Zusätzlich wird auch die wettbewerbsneutral tätige NRW.BANK aus dem Regelungsbereich für öffentliche Stellen ausgenommen. Sie erfüllt ihren Förderauftrag überwiegend im Hausbankenverfahren (private und genossenschaftliche Banken und Sparkassen) aber auch direkt, etwa mittels Darlehen oder Beteiligungen. Eine Gleichstellung mit den Hausbanken vereinfacht die Vertragsgestaltung, schafft Rechtssicherheit, spart Mehraufwände durch zusätzliche Vereinbarungen und bedeutet im Einzelfall mehr Klarheit. Gleichwohl erfolgt keine uneingeschränkte Verweisung auf das Bundesdatenschutzgesetz: Die in Absatz 4 benannten Stellen sind den Vorschriften für besondere Verarbeitungssituationen im Anwendungsbereich der DSGVO (§§ 15 bis 29) unterworfen. Gleichwohl ist die LDI Aufsichtsbehörde für derlei Verar-

beitungen. Insoweit wird dem öffentlichen Charakter dieser „Unternehmen“ Rechnung getragen. Wegen der Gleichstellung zu privaten Wettbewerbern gilt nur für derlei „Unternehmen“ die Bußgeldvorschrift des § 32 i.V.m. Artikel 83 DSGVO.
Absatz 1 Satz 3 erfasst auch Fälle einer mittelbaren Staatsverwaltung, in denen der Staat hoheitliche Aufgaben an natürliche Personen, juristische Personen des Privatrechts oder rechtsfähige Vereinigungen übertragen hat. Diese nehmen die übertragene Aufgabe im eigenen Namen wahr (bspw. öffentlich bestellte Vermessungsingenieure). Diese sog. Beliehenen sind öffentliche Stellen im funktionalen Sinn (vgl. hierzu etwa auch § 2 Absatz 4 IFG NRW).

Soweit diese Stellen personenbezogene Daten nicht für wirtschaftliche Zwecke verarbeiten, gilt ergänzend zur DSGVO Teil 2 des DSG NRW, beispielsweise bei der Datenverarbeitung im Beschäftigungskontext nach § 17 DSG NRW.

Zu Absatz 5

Absatz 5 entspricht dem § 2 Absatz 3 DSG NRW a.F. Sofern die Verarbeitung personenbezogener Daten im bereichsspezifischen Landesrecht gesondert geregelt ist, sind diese Vorschriften wie bisher gegenüber dem Teil 2 des DSG NRW vorrangig anzuwenden. Dem DSG NRW kommt somit nach wie vor nur eine subsidiäre Geltung zu und es bleibt insoweit Auffanggesetz. Satz 2 trägt der Möglichkeit Rechnung, dass die Vielzahl bereichsspezifischer Datenschutzvorschriften unter Umständen nicht abschließend ist und vermeidet so, durch Anwendbarkeit dieses Gesetzes in derlei Fällen, Regelungslücken.

Zu Absatz 6

Die DSGVO regelt nicht alle Bereiche der Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes. Mit Absatz 6 wird sichergestellt, dass für jegliche Verarbeitung personenbezogener Daten durch öffentliche Stellen ein einheitlicher Rechtsrahmen gilt, soweit nicht in Spezialvorschriften Abweichendes geregelt ist.
Im Einzelnen betrifft dies insbesondere folgende Bereiche:
a) Datenverarbeitung in Akten, die nicht dem Anwendungsbereich der DSGVO unterfallen.
Während Akten und Aktensammlungen, die nach bestimmten Kriterien geordnet sind, in den Anwendungsbereich der DSGVO fallen (Erwägungsgrund 15), werden vom Anwendungsbereich der DSGVO nicht erfasst die Datenverarbeitung in unstrukturierten Akten (vgl. Artikel 2 Absatz 1 DSGVO). Auch diese Verarbeitungen sollen innerhalb eines einheitlichen Rechtsrahmens erfolgen. Durch die entsprechende Anwendbarkeit der DSGVO, soweit keine Ausnahmen geregelt sind, wird dies sichergestellt.
b) Datenverarbeitungen, die nicht dem Anwendungsbereich des EU-Rechts unterfallen (Artikel 2 Absatz 2 Buchstabe a) DSGVO (z.B. Verfassungsschutzbehörde).
Durch die entsprechende Anwendung der DSGVO bei Vorrang des Spezialrechts wird auch für diese Bereiche sichergestellt, dass im Grundsatz die für alle öffentlichen Stellen geltenden allgemeinen Rechtsvorschriften zur Anwendung kommen. Abweichungen sind wie bisher auch spezialgesetzlich zu regeln.
Satz 2 berücksichtigt, dass für Streitigkeiten über verbindliche Beschlüsse der Aufsichtsbehörde sowie zwischen der Aufsichtsbehörde und natürlichen Personen im unmittelbaren Anwendungsbereich der DSGVO § 20 BDSG gilt. Soweit der Aufsichtsbehörde jedoch Eingriffsbefugnisse in Bezug auf Datenverarbeitung übertragen werden, die außerhalb des Anwendungsbereichs der DSGVO liegen, ist es erforderlich eine Regelung zum gerichtlichen Rechtsschutz für die diesen Befugnissen unterliegenden öffentlichen Stellen zu treffen.

Kapitel 2 Grundsätze der Verarbeitung personenbezogener Daten

Begründung zu § 6 Automatisierte Abrufverfahren und regelmäßige Datenübermittlung

Der Schutz personenbezogener Daten bei automatisierten Verfahren, welche die Übermittlung personenbezogener Daten durch Abruf (Online-Abrufe) oder die regelmäßige Datenübermittlung (Absatz 4) zulassen, soll unter Ausnutzung der Öffnungsklausel in Artikel 6 Absätze 2 und 3 DSGVO durch die Vorschrift wie bisher bereits auf den Zeitpunkt der Einrichtung bzw. Absprache derlei Verfahren vorverlegt werden. Da beide Verfahrensarten ein erhöhtes Risiko potenzieller Gefährdungen des Persönlichkeitsrechts in sich bergen, soll so ein angemessenes Schutzniveau für den Kreis der von solchen Verfahren betroffenen Personen erreicht werden. Die Vorschrift ist § 9 DSG NRW a.F. nachgebildet.

Durch die Verordnungsermächtigung nach Absatz 2 werden die Ministerien entsprechend dem Ressortprinzip ermächtigt, für die öffentlichen Stellen ihres Geschäftsbereiches die Einrichtung von Online-Verfahren durch Rechtsverordnung zuzulassen. Die Verordnungsermächtigung steht unverändert unter dem Vorbehalt der Abwägung. Das mit der Einrichtung automatisierter Verfahren einhergehende potenzielle Gefährdungsmoment des betroffenen Personenkreises muss in angemessener Relation zu der beabsichtigten technischen Aufgabenerledigung der öffentlichen Stelle stehen. Die Vorschrift genügt damit auch dem Grundsatz der Verhältnismäßigkeit, da die Aufgabenzuweisung der öffentlichen Stelle selbst nicht aus der Ermächtigung folgt; diese muss durch eine andere Rechtsnorm gegeben sein.

Für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle gilt § 6 demgegenüber naturgemäß nur in Teilen. Das entspricht der bisherigen Rechtslage nach § 9 Absatz 4 DSG NRW a.F.

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

Die DSGVO enthält keine Regelungen zur Information von dritten Personen und nicht-öffentlichen Stellen über die Verwendung der bei diesen erhobenen Daten. Entsprechend der bisher geltenden Vorschrift (§ 12 Absatz 3 DSG NRW a.F.) soll eine solche Informationspflicht auch zukünftig normiert werden, um auch gegenüber einer dritten Person oder nicht-öffentlichen Stelle, bei der Daten erhoben werden sollen, ein größtmögliches Maß an Transparenz herzustellen (siehe auch Artikel 5 Absatz 1 Buchstabe a DSGVO). Die Regelungsbefugnis ergibt sich aus Artikel 6 Absätze 2 und 3 DSGVO, indem eine Maßnahme zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung geregelt wird.

Begründung zu § 8 Verantwortung für die Datenübermittlung

Im DSG NRW wird es künftig keine speziellen Vorschriften zur Übermittlung personenbezogener Daten geben. Die Verantwortlichkeit im Rahmen einer Übermittlung personenbezogener Daten richtet sich, soweit sie nicht spezialgesetzlich geregelt ist, nach § 8 DSG NRW. Gemäß dem bisherigen Recht soll die Verantwortlichkeit für die Übermittlung personenbezogener Daten aber fixiert werden. Die Regelungsbefugnis hierzu ergibt sich aus Artikel 4 Nummer 7 DSGVO.

§ 8 entspricht § 14 Absatz 2 DSG NRW a.F. Nach Artikel 5 Absatz 2 DSGVO ist die übermittelnde Stelle für die Einhaltung der Datenschutzgrundsätze verantwortlich und nachweispflichtig, damit ist sie auch für die Zulässigkeit der Übermittlung verantwortlich. Abweichend hiervon wird im Falle eines Ersuchens durch eine öffentliche Stelle die Verantwortung auf diese übertragen.

Begründung zu § 9 Zulässigkeit der Datenverarbeitung im Hinblick auf die Zweckbindung

Zu Absatz 1

Absatz 1 bestimmt entsprechend der bisherigen Regelung des § 13 Absatz 3 DSG NRW a.F., dass eine Verarbeitung zu den genannten Zwecken keine zweckändernde Datenverarbeitung ist, sondern diese Zwecke jeder Datenverarbeitung immanent sind und eine diesbezügliche Verarbeitung ggf. unter den in diesem Absatz genannten Beschränkungen zulässig ist. Die Befugnis für eine solche Regelung ergibt sich aus Artikel 6 Absätze 2 und 3 DSGVO. Danach dürfen im mitgliedstaatlichen Recht die Zwecke der Verarbeitung bestimmt werden.

Zu Absatz 2

Artikel 6 Absatz 4 Fall 2 DSGVO eröffnet einen Regelungsspielraum für die Mitgliedsstaaten in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist. Sie können Rechtsvorschriften erlassen, die in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele darstellen. Mit den Absätzen 2 und 4 wird von dieser Möglichkeit Gebrauch gemacht. Sie spiegeln im Wesentlichen die Regelungen des § 13 Absatz 2 DSG NRW a.F. wider, soweit sie nicht durch die DSGVO selbst geregelt werden.

Im Einzelnen werden die Tatbestände des Absatzes 2 im Schwerpunkt auf folgende Normen der DSGVO gestützt:

Nummer 1.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben c) und e)
Nummer 2.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben i) Atl. 2
Nummer 3.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben d) und e)
Nummer 4.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben e)
Nummer 5.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben i) Alt. 2 und j)
Nummer 6.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben e) und i)
Nummer 7.: Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben e), Artikel 89.

Zu Absatz 3

Gemäß Artikel 23 Absatz 1 DSGVO können die Rechte und Pflichten gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5 beschränkt werden, soweit dies erforderlich ist, um die in Artikel 23 Absatz 1 Buchstaben a) bis j) genannten Aspekte sicherzustellen und die Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. In den Fällen, in denen eine zweckändernde Verarbeitung auf der Grundlage von Artikel 6 Absatz 4 Fall 2 in Verbindung mit Artikel 23 Absatz 1 zugelassen wurde, wird zur Absicherung der Erfüllung dieser Zwecke normiert, dass eine Information der betroffenen Person nicht erfolgt, soweit und solange der Zweck der Verarbeitung durch eine solche Information gefährdet würde. Die Ausnahme von der Informationspflicht wird auf dieselben oben zu Absatz 2 aufgeführten Buchstaben des Artikels 23 Absatz 1 DSGVO gestützt wie die Zulässigkeit der Zweckänderung.
Die Ausnahme von der Informationspflicht besteht nur solange eine Gefährdung des Verarbeitungszwecks besteht. Besteht die Gefährdung nicht mehr, hat die Information der betroffenen Person zu erfolgen.

Zu Absatz 4

Absatz 4 regelt die Fälle der Zulässigkeit eine Zweckänderung zum Schutz der betroffenen Person. Die Tatbestände stützen sich auf Artikel 6 Absatz 4 Fall 2 i.V.m. Artikel 23 Absatz 1 Buchstaben i) Alternative 1 DSGVO. Anders als bei Absatz 2 i.V.m. Absatz 3 wird bei diesen Zweckänderungen keine Ausnahme von der Informationspflicht gemacht.

Zu Absatz 5

Absatz 5 ist angelehnt an den § 13 Absatz 2 Satz 3 DSG NRW a.F. Soweit die personenbezogenen Daten einem Berufsgeheimnis oder besonderen Amtsgeheimnis unterliegen, ist eine Zweckänderung nach den Absätzen 2 und 4 nicht zulässig.
Die Regelungsbefugnis ergibt sich aus Artikel 6 Absatz 2 und Absatz 3 Satz 3 DSGVO, welcher regelt, welcher Zweckbindung bestimmte Daten unterliegen. Dementsprechend wird eine Ausnahme von den zulässigen Zweckänderungsfallgruppen geregelt. Die Zulässigkeit einer Zweckänderung auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 4 Fall 1 DSGVO bleibt hingegen auch hier unberührt.

Zu Absatz 6

Absatz 6 stellt sicher, dass die an öffentliche oder nicht-öffentliche Stellen u.a. auf Anforderung übermittelten Daten nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden, und entspricht dem § 14 DSG NRW a.F. Bei der Übermittlung an nicht-öffentliche Stellen verbleibt es nach Satz 2 bei der Hinweispflicht der übermittelnden Stelle, die insoweit § 16 Absatz 2 DSG NRW a.F. nachgebildet ist. Absatz 6 dieses Gesetzes ist eine Rechtsgrundlage im Sinne des Artikel 6 Absatz 3 Buchstabe b DSGVO und gleichzeitig eine Maßnahme im Sinne von Artikel 23 Absatz 2 DSGVO. Absatz 6 dient auch dem Schutz der Rechte der betroffenen Person.

Zu Absatz 7

Absatz 7 bildet die Übermittlung personenbezogener Daten an öffentlich-rechtliche Religionsgesellschaften nach dem Vorbild des § 15 DSG NRW a.F. ab. Um dabei ein einheitliches Datenschutzniveau mit der Übermittlung an öffentliche Stellen nach diesem Gesetz zu gewährleisten, muss der Empfänger sichergestellt haben, dass ausreichende Datenschutzmaßnahmen getroffen sind. Im Sinne des Artikels 91 DSGVO betrifft das insbesondere die eigenen Datenschutzgesetze der Religionsgesellschaften (bspw. DSG EKD und KDG), die mit der DSGVO in Einklang stehen müssen.

Begründung zu § 10 Löschung personenbezogener Daten

Zu Absatz 1

Die Norm ist angelehnt an den § 19 Absatz 4 DSG NRW a.F. Sie soll sicherstellen, dass (rechtmäßig gespeicherte) personenbezogene Daten vor ihrer Löschung den jeweiligen Archiven angeboten werden. Die Regelungsbefugnis für diese Modifikation im Zusammenhang mit Löschungspflicht ergibt sich aus Artikel 6 Absatz 2 i.V.m. Artikel 17 Absatz 3 Buchstabe d DSGVO, wonach personenbezogene Daten nicht zu löschen sind, wenn ansonsten im öffentlichen Interesse liegende Archivzwecke unmöglich gemacht oder ernsthaft beeinträchtigt würden.

Zu Absatz 2

Die Sätze 1 und 2 schränken die Rechte des Betroffenen und die Pflicht des Verantwortlichen aus Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 ein. Dabei wird von der Öffnungsklausel des Artikel 23 Absatz 1 lit. e) Gebrauch gemacht. Die in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen bleiben unberührt. Hierdurch wird unter bestimmten in der Norm genannten Voraussetzungen eine Ausnahme von der Löschungsverpflichtung vorgesehen. Diese Ausnahme ist beschränkt auf die nicht automatisierte Datenverarbeitung und setzt neben einem unverhältnismäßig hohen Aufwand der Löschung voraus, dass das Interesse der betroffenen Person an der Löschung personenbezogener Daten als gering anzusehen ist. Eine solche Ausnahme ist geboten im Sinne der Funktionsfähigkeit der öffentlichen Stellen. Im Interesse des Datenschutzes tritt an die Stelle der Löschung die Einschränkung der Verarbeitung (Artikel 18 der Verordnung (EU) 2016/679). Artikel 18 Absatz 2 und 3 sowie 19 der Verordnung (EU) 2016/679 vermitteln effektive Garantien gegen Missbrauch und unrichtige Übermittlung im Sinne des Artikels 23 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679. Die Einschränkung von der Zwangslöschung gilt nicht für die Fallgruppe des Artikels 17 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679, da der Verantwortliche bei einer unrechtmäßigen Datenverarbeitung nicht schutzwürdig ist und sich nicht auf einen unverhältnismäßig hohen Aufwand der Löschung wegen der von ihm selbst gewählten Art der Speicherung berufen kann.

Kapitel 3 Rechte der betroffenen Personen

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

Zu Absatz 1

Die DSGVO sieht in ihren Artikel 13 und 14 umfängliche Informationspflichten des Verantwortlichen gegenüber der betroffenen Person bei der Erhebung personenbezogener Daten sowie etwaigen zweckändernden Weiterverarbeitungen vor. Auf diese Weise soll ein größtmögliches Maß an Transparenz (Artikel 12 DSGVO, Grundsatz der Transparenz) hergestellt und die betroffenen Personen in die Lage versetzt werden, ihre Rechte umfassend wahrzunehmen. Artikel 12 DSGVO unterscheidet aber Informationen nach solchen für die Öffentlichkeit und Informationen, die nur für die betroffene Person bestimmt sind. So können etwa für die Öffentlichkeit bestimmte Informationen durch den Verantwortlichen auch in elektronischer Form, insbesondere auf einer Website, bereitgestellt werden (Erwägungsgrund 58 zu Artikel 12 DSGVO).

Das Recht der betroffenen Person auf Information über die Datenverarbeitung der sie betreffenden personenbezogenen Daten darf allerdings nur unter engen Voraussetzungen beschränkt werden. Artikel 23 Absatz 1 DSGVO gibt den Maßstab für derartige Beschränkungen vor.
Im Einzelnen werden die Tatbestände des Absatz 1 im Schwerpunkt auf folgende Normen der DSGVO gestützt:
Nummer 1: Artikel 23 Absatz 1 Buchstabe c), d), e) und g)
Nummer 2: Artikel 23 Absatz 1 Buchstabe e) und i)
Nummer 3: Artikel 23 Absatz 1 Buchstabe j).

Die oder der Verantwortliche hat zu prüfen, in welchen Umfang und in welchem Zeitraum eine entsprechende Gefährdung besteht, die die Beschränkung rechtfertigt. Liegt eine Gefährdung nicht mehr vor, ist die entsprechende Information zu erteilen.

Unberührt bleiben die in Artikel 13 Absatz 4 sowie Artikel 14 Absatz 5 DSGVO normierten Ausnahmen von der Informationspflicht.

Zu Absatz 2

Für den Fall, dass personenbezogene Daten an die in Absatz 2 genannten Behörden übermittelt wurden oder von diesen Stellen an die öffentliche Stelle übermittelt werden, regelt Absatz 2, dass die beabsichtigte Information der betroffenen Person über den Übermittlungsvorgang erst nach ausdrücklicher Zustimmung der ebenfalls betroffenen Behörde erteilt werden darf. Die Regelung dient präventiv dem Ausschluss von Kollisionen mit gesetzlichen Strafverfolgungs- oder Sicherheitsbelangen des Staates. Die Beschränkung in Absatz 2 wird im Schwerpunkt auf Artikel 23 Absatz 1 Buchstabe a) - e) gestützt.

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

Zu Absatz 1

Die Regelung dient dem Erhalt der behördlichen Funktionsfähigkeit im Sinne eines Ausuferungsschutzes und beruht auf Erwägungsgrund 63 DSGVO. Absatz 1 betrifft beispielsweise umfangreiche Patientenakten, in denen sich die Informationen über Jahre angesammelt haben und deren Durchforsten zeitintensive Recherchen des Verantwortlichen erforderlich machen würde. In solchen Fällen kann der Verantwortliche eine Präzisierung des Auskunftsverlangens, etwa auf bestimmte Diagnosen, Befunde oder genaue Zeiträume verlangen. Gleichwohl kann ein Verantwortlicher, wo möglich, das Auskunftsverlangen der betroffenen Person auslegen und die Auskunft auf diesen ermittelten Teil beschränken.

Zu Absatz 2

Satz 1 ist angelehnt an die Beschränkungen des § 18 Absatz 3 DSG NRW a.F. Das Recht auf Auskunft nach Artikel 15 DSGVO darf nur unter den engen Voraussetzungen von Artikel 23 Absatz 1 DSGVO beschränkt werden.
Die Beschränkungen des Auskunftsrechts sind weitgehend identisch mit den Beschränkungen der Informationspflicht in § 11 und werden auf dieselben oben aufgeführten Tatbestände des Artikel 23 Absatz 1 DSGVO gestützt.
Der Verantwortliche hat zu prüfen, in welchem Umfang und für welchen Zeitraum eine entsprechende Gefährdung besteht. Liegt eine Gefährdung nicht mehr vor, ist die entsprechende Auskunft zu erteilen.
Satz 2 nimmt bestimmte Daten von der Verpflichtung zur Auskunftserteilung aus. Das gilt zunächst für sog. Sicherungsdaten, also Daten, die aus Gründen der Datensicherung nicht gelöscht werden dürfen und deshalb bei der öffentlichen Stelle noch gespeichert werden. Gleiches gilt für Daten, die lediglich für die Datenschutzkontrolle gesichert werden. Beide Fälle dienen der technischen Absicherung der Funktionsfähigkeit der jeweiligen Behörde. Dieser Sachverhalt stellt für die betroffene Person keine wesentliche Beeinträchtigung und somit auch keinen auskunftspflichtigen Tatbestand dar. Den Interessen der betroffenen Person wird dadurch Rechnung getragen, dass die öffentliche Stelle zum Schutze vor zweckfremden Verarbeitungen angemessene technische und organisatorische Maßnahmen getroffen hat. Gleiches gilt für Sicherheitskopien die bei Auftragsverarbeitern gespeichert werden.

Zu den Absätzen 3 und 4

Für den Fall, dass personenbezogene Daten an die in Absatz 4 genannten Behörden übermittelt wurden oder von diesen Stellen an die öffentliche Stelle übermittelt wurden, regelt Absatz 4, dass die beabsichtigte Information auf Nachfrage der betroffenen Person über den Übermittlungsvorgang erst nach ausdrücklicher Zustimmung der ebenfalls betroffenen Behörde erteilt werden darf. Die Regelung dient, ebenso wie Absatz 5, damit neben § 11 Absatz 2 DSG NRW präventiv dem Ausschluss von Kollisionen mit gesetzlichen Strafverfolgungs- oder Sicherheitsbelangen des Staates. Die Beschränkung in Absatz 4 wird im Schwerpunkt auf Artikel 23 Absatz 1 Buchstabe a) - e) gestützt. Um eine spätere Überprüfung der Entscheidung zu ermöglichen, sind die Gründe für die Ablehnung der Auskunftserteilung aufzuzeichnen.

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

Das Recht der betroffenen Person auf und damit zugleich die Pflicht des Verantwortlichen zur Information der betroffenen Person bei einer Verletzung des Schutzes ihrer personenbezogenen Daten nach Artikel 34 DSGVO darf nur unter den engen Voraussetzungen von Artikel 23 Absatz 1 DSGVO beschränkt werden.
Die Nummern 1 und 2 entsprechen den Beschränkungen aus den § 11 und § 12 und werden auf dieselben Tatbestände des Artikels 23 Absatz 1 DSGVO gestützt.
Die Verhinderung von Gefährdungen der Sicherheit von IT-Systemen gehört ebenso zu den wichtigen öffentlichen Zielen im Sinne von Artikel 23 Absatz 1 Buchstabe e DSGVO. Unter IT-Systemen werden dabei sowohl Hardwarekomponenten als auch Software in jeglicher Hinsicht verstanden.
Der Verantwortliche hat zu prüfen, in welchen Umfang und in welchem Zeitraum eine entsprechende Gefährdung besteht. Liegt eine Gefährdung nicht mehr vor, hat die entsprechende Information zu erfolgen.
Unberührt bleiben die in Artikel 34 Absatz 3 DSGVO geregelten Ausnahmen von der Benachrichtigungspflicht.

Begründung zu § 14 Beschränkung des Widerspruchsrechts

§ 14 schränkt das Recht auf Widerspruch nach Artikel 21 Absatz 1 DSGVO ein, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 14 setzt öffentliche Interessen des Verantwortlichen im Sinne des Artikel 23 Absatz 1 Buchstabe e) DSGVO voraus, die im konkreten Einzelfall zwingend sein müssen und Vorrang vor den Interessen der betroffenen Person haben. Darüber hinaus ist das Recht auf Widerspruch ausgeschlossen, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 17 Absatz 4 enthält spezifische Einschränkungen des Widerspruchsrechts für die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und statistischen Zwecken.

Kapitel 4 Vorschriften für besondere Verarbeitungssituationen

Begründung zu § 15 Garantien zum Schutz personenbezogener Daten und anderer Grundrechte

§ 15 setzt das Erfordernis aus Artikel 9 Absatz 2 Buchstabe b, g und j DSGVO um, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ zu regeln. Die Regelung wird im Kapitel IV vorangestellt, da in jeder der in diesem Abschnitt geregelten besonderen Verarbeitungssituationen auch besondere Kategorien personenbezogener Daten verarbeitet werden können. In diesen Fällen sind immer dem Risiko der Verarbeitung dieser Daten entsprechende Schutzmaßnahmen für die Rechte der betroffenen Personen gegenüberzustellen. Durch Nummer 5 in Verbindung mit § 4 (Begriffsbestimmung) dieses Gesetzes wird das Datenschutzniveau des DSG NRW a.F. aufrechterhalten.
§ 15 regelt ausschließlich diejenigen Schutzmaßnahmen, die im Bereich des allgemeinen Datenschutzes zu treffen sind. Im Übrigen sind entsprechende Garantien zur Wahrung der Grundrechte des Betroffenen im bereichsspezifischen Datenschutzrecht festzulegen. Sofern bereichsspezifische Regelungen aber unvollständig sind oder gänzlich fehlen, greift § 5 Absatz 5 Satz 2 dieses Gesetzes als Auffangnorm.

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

Begründung zu § 16 Verarbeitung besonderer Kategorien personenbezogener Daten

Zu Absatz 1

§ 16 Absatz 1 regelt die Fälle, in denen die Verarbeitung besonderer Kategorien personenbezogener Daten ohne die Einwilligung der betroffenen Person aus Gründen eines erheblichen öffentlichen Interesses zulässig ist. Nach Artikel 9 Absatz 2 Buchstabe g und h DSGVO können die Mitgliedstaaten die Verarbeitung im erheblichen öffentlichen Interesse durch Gesetz zulassen. Von dieser Öffnungsklausel wurde in allgemeiner Form Gebrauch gemacht, spezifische Maßnahmen sind im Fachrecht vorzusehen. Gleiches gilt für die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit nach Artikel 9 Absatz 2 Buchstabe i DSGVO (§ 16 Satz 1 Nummer 3).
Mit § 16 Nummer 4 wird von der Öffnungsklausel des Artikel 9 Absatz 2 Buchstabe b DSGVO Gebrauch gemacht, insbesondere um zu gewährleisten, dass öffentliche Stellen, die Versorgungsleistungen erbringen, die für ihre Aufgabenwahrnehmung erforderliche Datenverarbeitung durchführen können, beispielsweise in Bezug auf Versorgungsleistungen und auf Beihilfeansprüche gegen den Dienstherren u.a. in Krankheitsfällen.

Zu Absatz 2

Absatz 2 regelt in Ausformung von Artikel 9 Absatz 4 DSGVO die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten in welche die betroffene Person eingewilligt hat (Artikel 9 Absatz 2 Buchstabe a DSGVO). Wegen der besonderen Sensibilität dieser Daten sind derlei Verarbeitungen nur mit schriftlicher Einwilligung der betroffenen Person zulässig. Das dient einerseits der Beweisfunktion des Artikels 7 Absatz 1 DSGVO und andererseits wird hierdurch eine Warnfunktion gegenüber der betroffenen Person etabliert.

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

§ 17 regelt die spezifischen Anforderungen an die Verarbeitung personenbezogener Daten für Forschungs- und Statistikzwecke. Die Datenverarbeitung zu Forschungs- und Statistikzwecken genießt in Artikel 89 DSGVO eine Privilegierung; zusätzlich wird eine Datenverarbeitung zu Forschungs- und Statistikzwecken außerhalb des Bereichs besonderer Kategorien von der grundrechtlich garantierten Forschungsfreiheit im Grundsatz erlaubt.
Die Regelungsbefugnis für diesen Paragrafen ergibt sich aus Artikel 6 Absätze 2 und 3 in Verbindung mit Artikel 89 DSGVO. Gleichzeitig wird von der Ermächtigung aus Artikel 9 Absatz 2 Buchstabe j DSGVO Gebrauch gemacht und die Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken geregelt. Nach Artikel 9 Absatz 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Artikel 9 Absatz 2 der Verordnung sieht Ausnahmen von diesem Verbot vor. Die Ausnahmen ergeben sich teilweise unmittelbar aus der Verordnung selbst, z.B. die ausdrückliche Einwilligung nach Artikel 9 Absatz 2 Buchstabe a DSGVO. Für die Verarbeitung besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke ohne Einwilligung der betroffenen Person bedarf es einer nationalen Regelung (auf Basis von Artikel 9 Absatz 2 Buchstabe j DSGVO).

Zu Absatz 1

Absatz 1 normiert wie die bisherige Regelung des § 28 Absatz 1 DSG NRW a.F. das Datenschutzniveau im Sinne eines Rangverhältnisses von Anonymisierung vor Pseudonymisierung vor Forschung mit nicht pseudonymisierten Daten.

Zu Absatz 2

Absatz 2 regelt die Fälle, in denen eine Verarbeitung auch ohne Einwilligung der betroffenen Person zulässig ist.

Zu Absatz 3

Absatz 3 übernimmt die bisherigen Vorschriften zum Schutz der Rechte der betroffenen Personen, er ist angelehnt an § 28 Absatz 3 DSG NRW a.F. Durch die Vorgaben zur Anonymisierung und zu der getrennten Speicherung der Merkmale, mit denen Einzelangaben bestimmten Personen zugeordnet werden können, werden geeignete Mittel zur Wahrung der Rechte und Freiheiten der betroffenen Person im Sinne des Artikels 89 Absatz 1 DSGVO vorgesehen.

Zu Absatz 4

Absatz 4 spezifiziert die Verarbeitung (Übermittlung) personenbezogener Daten im Hinblick auf deren Veröffentlichung, indem zum Schutz der Rechte der betroffenen Personen nur im besonderen Ausnahmefall eine personenbezogene Darstellung der Forschungsergebnisse zugelassen wird. Dies soll nur zulässig sein, wenn dies für die Darstellung von Ereignissen der Zeitgeschichte erforderlich ist und eine Abwägung der öffentlichen Interessen mit den schutzwürdigen Belangen der betroffenen Person zu dem Ergebnis kommt, dass das öffentliche Interesse die schutzwürdigen Belange erheblich überwiegt.

Zu Absatz 5

Absatz 5 regelt im Einklang mit Artikel 89 Absatz 2 und Artikel 14 Absatz 5 DSGVO, unter welchen Voraussetzungen die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch nicht bestehen. Hierdurch soll gewährleistet werden, dass unter den Voraussetzungen des Absatzes 1 zulässige im öffentlichen Interesse liegende Forschungs- und Statistikvorhaben nicht durch die Wahrnehmung von Betroffenenrechten gefährdet werden. Dies entspricht der in der DSGVO angelegten Privilegierung der Forschung und Statistik.

Zu Absatz 6

Absatz 6 regelt die Datenübermittlung an Empfänger, auf die das DSG NRW keine Anwendung findet. Die Übermittlung ist nur zulässig, soweit sich die Empfänger verpflichten, die Daten nur für das von ihnen bezeichnete Forschungs- oder Statistikvorhaben zu verwenden und die in den Absätzen 2 und 3 normierten Garantien zum Schutz der Rechte der betroffenen Personen zu beachten. Dadurch wird gewährleistet, dass auch für Datenempfänger außerhalb des Anwendungsbereiches dieses Gesetzes die in den Absätzen 2 und 3 normierten Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne des Artikels 89 Absatz 1 DSGVO gelten. Im Übrigen wird das Datenschutzniveau nach § 28 Absatz 5 DSG NRW a.F. aufrechterhalten.

Begründung zu § 18 Datenverarbeitung im Beschäftigungskontext

Artikel 88 DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifische Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigungskontext zu schaffen, wovon auch das Ausbildungsverhältnis umfasst ist. Hinsichtlich der Verarbeitung besonderer Datenkategorien in diesem Zusammenhang enthält Artikel 9 Absatz 2 Buchstabe b DSGVO eine Öffnungsklausel für Regelungen der Mitgliedstaaten für spezielle Verarbeitungszwecke. Von diesen Regelungsbefugnissen wird unter Beibehaltung des in § 29 DSG NRW a.F. normierten Standards und unter Spezifikation der Verarbeitung besonderer Kategorien personenbezogener Daten Gebrauch gemacht. Die Absätze 2, 3, 4, 5, 6, 7 des § 29 DSG NRW a.F. wurden im Wesentlichen beibehalten.

Zu Absatz 1

Seit der Entscheidung des Bundesarbeitsgerichts vom 11.12.2014 (8 AZR 1010/13) ist die in Rechtsprechung und Literatur umstrittene Frage geklärt, dass Beschäftigtendaten auch auf der Grundlage einer wirksamen Einwilligung nach § 4 Absatz 1 BDSG (entspricht § 4 Absatz 1 DSG NRW a.F.) erhoben werden dürfen. Die tragenden Erwägungen der Entscheidung des Bundesarbeitsgerichts, die zu § 32 BDSG ergangen ist, dürften auf das Landesdatenschutzrecht entsprechende Anwendung finden. Denn auch innerhalb des öffentlichen Bereichs kann sich ein entsprechendes Bedürfnis für eine Datenübermittlung auf Grundlage einer Einwilligung ergeben. Zu denken ist beispielsweise an die Bekanntgabe von personenbezogenen Daten im Rahmen eines behördlichen Intranets oder aber generell bei der freiwilligen Übermittlung von Daten durch Beschäftigte.

Zu Absatz 2

Absatz 2 trägt der Besonderheit des Beschäftigungsverhältnisses als Abhängigkeitsverhältnis und der daraus resultierenden Situation der Beschäftigten Rechnung. Es handelt sich ebenfalls um eine spezifischere Vorschrift im Sinne von Artikel 88 Absatz 1 der Verordnung (EU) 2016/679. Nach Erwägungsgrund 155 der Verordnung (EU) 2016/679 können insbesondere

Vorschriften über die Bedingungen erlassen werden, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden dürfen.
Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, sind insbesondere die im Beschäftigungsverhältnis grundsätzlich bestehende Abhängigkeit der oder des Beschäftigten vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen. Neben der Art des verarbeiteten Datums und der Eingriffstiefe ist zum Beispiel auch der Zeitpunkt der Einwilligungserteilung maßgebend. Vor Abschluss eines (Arbeits-)Vertrages werden Beschäftigte regelmäßig einer größeren Drucksituation ausgesetzt sein, eine Einwilligung in eine Datenverarbeitung zu erteilen. Satz 2 legt fest, dass eine freiwillige Einwilligung insbesondere vorliegen kann, wenn die oder der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Die Gewährung eines Vorteils liegt beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen. Auch die Verfolgung gleichgerichteter Interessen spricht für die Freiwilligkeit einer Einwilligung. Hierzu zählt in Verbindung mit § 16 insbesondere der Schutz des Beschäftigten vor unberechtigter Strafverfolgung durch Aufnahme in eine DNA-Referenzdatei zum Ausschluss von Trugspuren. Auch kann etwa die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet dazu zählen, bei der Arbeitgeber und Beschäftigter im Sinne eines betrieblichen Miteinanders zusammenwirken. Als formelle Voraussetzung einer Einwilligung ist grundsätzlich die Schriftform angeordnet, um die informationelle Selbstbestimmung der betroffenen Beschäftigten abzusichern. Damit wird die Nachweispflicht des Arbeitgebers im Sinne von Artikel 7 Absatz 1 der Verordnung (EU) 2016/679 konkretisiert. Hinzu kommt die Pflicht des Arbeitgebers zur Aufklärung in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch den Beschäftigten sowie dessen Folgen nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679.

Zu Absatz 3

Absatz 3 dient (neben § 16 Absatz 1 Nr. 4) der Umsetzung von Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Im Einklang mit der Verordnung ist eine Verarbeitung besonderer Kategorien personenbezogener Daten zu Beschäftigungszwecken 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. Die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses kann auch die Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit einschließen. Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke bleibt unberührt; zum Beispiel richtet sich diese im Fall der Verarbeitung zu Zwecken der Gesundheitsvorsorge nach § 16 Absatz 1 Nummer 3. Sollte eine Verarbeitung zugleich mehreren Zwecken dienen, gilt für den jeweiligen Zweck die jeweils einschlägige Verarbeitungsgrundlage. Neben der Verhältnismäßigkeitsprüfung im Rahmen der Erforderlichkeit darf wie bisher nach § 28 Absatz 6 BDSG a. F. kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen der Betroffenen die Interessen der Verantwortlichen an der Verarbeitung überwiegen. Die Vorschriften des Absatzes 2 gelten auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten, wie z.B. von Gesundheitsdaten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. An die Freiwilligkeit einer Einwilligung in die Datenverarbeitung besonderer Kategorien personenbezogener Daten sind strenge Anforderungen zu stellen.

Zu Absatz 4

Aufgrund der Entwicklung der Sicherheitslage in Europa und in der Bundesrepublik Deutschland liegt ein Ausschluss von Sicherheitsbedenken durch den Einsatz der Bewerberinnen und Bewerber vor der Einstellung bzw. Verwendung im öffentlichen Interesse. Es sind daher für die Zukunft auch entsprechende Überprüfungen der Rechts- und Verfassungstreue der Bewerberinnen und Bewerber zu ermöglichen. Zudem ist eine erhöhte Beschäftigung von Regierungsbeschäftigten in der Polizei in einem deutlich erweiterten Umfang vorgesehen.

Es werden auch bereits aktuell in den Polizeibehörden Regierungsbeschäftigte in unterschiedlichen - auch mit erhöhten Sicherheitserfordernissen versehenen - Bereichen eingesetzt. Erfasst werden sollen schließlich auch privatrechtliche Ausbildungs- und Praktikantenverhältnisse, die ebenfalls in den Polizeibehörden vorkommen und bei denen Sicherheitsrisiken ebenfalls ausgeschlossen werden sollen. Die Norm verwendet in Bezug auf Praktikanten den ebenfalls in § 1 TV Prak-L sowie vom Bundesarbeitsgericht (vgl. BAG, Urteil vom 13.03.03, 6 AZR 564/01) verwendeten Terminus „Praktikantenverhältnis“. Der Satz 1 enthält die notwendige Übermittlungsbefugnis, Satz 2 konkretisiert die Verarbeitung der übermittelten Daten.

Für die Verfassungsschutzbehörde, die aus europarechtlichen Gründen vom Anwendungsbereich des Datenschutzgesetzes NRW ausgenommen ist, wird ein Mitwirkungstatbestand im Sinne des § 3 Absatz 4 Verfassungsschutzgesetz NRW geschaffen.

Zu Absatz 5

Der Absatz behält die Regelung des § 29 Absatz 2 DSG NRW a.F. bei und stellt sicher, dass eine Gleichbehandlung von nicht beamteten Beschäftigten und Beamten des Landes in datenschutzrechtlicher Sicht gewährleistet wird.

Zu den Absätzen 6 und 7

Absatz 6 entspricht dem § 29 Absatz 3 DSG NRW a.F. Er soll der Besonderheit von Daten aus ärztlichen und psychologischen Untersuchungen und Tests, die zur Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben werden, Rechnung tragen und legt aufgrund dessen fest, dass eine Einwilligung nur schriftlich erfolgen kann. Das Schriftformerfordernis im Interesse der Betroffenen kann gem. Artikel 9 Absatz 4 DSGVO geregelt werden.
Absatz 7 entspricht dem § 29 Absatz 4 DSG NRW a. F. Er enthält in Satz 1 eine Zwangslöschung der Daten, sobald feststeht, dass das Dienst- oder Arbeitsverhältnis nicht zustande kommt. Die Löschungsverpflichtung betrifft insbesondere auch die Bewerbungsunterlagen der betroffenen Person. Zugleich legt Satz 1 fest, wann diese Löschung ausnahmsweise nicht zu erfolgen hat. Dies ist der Fall, wenn eine entsprechende Einwilligung vorliegt oder wenn Fristen nach dem AGG abzuwarten sind, wie etwa die Zweimonatsfrist für Ansprüche auf Entschädigung und Schadenersatz nach § 15 AGG oder die Dreimonatsfrist des § 61b ArbGG, innerhalb der geklagt werden kann.
In Satz 2 wird auch das Prinzip der Zwangslöschung von Daten, die im Falle eines beendeten Dienst- oder Arbeitsverhältnisses nicht mehr benötigt werden, fortgeführt.

Zu den Absätze 8, 9 und 10

Absatz 8 beschränkt die automatisierte Verarbeitung personenbezogener Daten auf die Fälle, die dem Schutz des Beschäftigten dienen. Er entspricht § 29 Absatz 5 DSG NRW a.F.
Absatz 9 verbietet eine Nutzung der Daten zu Zwecken der Verhaltens- und Leistungskontrolle und stimmt im Wesentlichen mit § 29 Absatz 6 DSG NRW a.F. überein.

Absatz 10 dient ebenfalls dem Schutz der Beschäftigten und ist identisch mit § 29 Absatz 7 DSG NRW a.F.

Zu Absatz 11

Mit dem Absatz 11 wird unter Berücksichtigung der vorgehenden Regelungen der DSGVO der bisherige § 29a Absatz 4 DSG NRW a.F. aufrecht gehalten. Damit wird auch die letzte Änderungen dieser Vorschrift durch das Gesetz vom 02. Juni 2015 (GVBl Nr. 27 vom 30. Juni 2015) insoweit bewahrt, weil sie eine sichere Rechtsgrundlage für den Einsatz der Ortungsfunktion des Digitalfunks bei den Sicherheitsbehörden darstellt. Die Befugnis zur ergänzenden Regelung zur DSGVO ergibt sich aus Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Absatz 2 DSGVO. Soweit Betroffenenrechte berührt sind, gelten auch hier die einschlägigen Vorschriften der DSGVO.

Der Justizvollzug nimmt ebenso wie die Polizei am BOS-Digitalfunk teil. Diese Technik wird auch in Justizvollzugsanstalten dazu genutzt, Bedienstete zu ihrer eigenen Sicherheit elektronisch zu orten, etwa bei Notlagen in der Anstalt. Das Gesetz sieht in § 18 Absatz 9 DSG NRW vor, dass Leitstellen und Befehlsstellen die bei dem Betrieb des Systems anfallenden Daten aus dienstlichen Gründen zur Sicherheit der Einsatzkräfte verarbeiten dürfen.

Die Vorschrift des § 18 Absatz 11 DSG NRW regelt einen Spezialfall einer erforderlichen organisatorischen Maßnahme im Beschäftigungskontext; andere Systeme zur Überwachung des Aufenthaltsortes mittels mobiler technischer Mittel, die nicht auf der BOS-Digitalfunktechnik beruhen, können weiterhin gemäß § 18 Absatz 1 Satz 1 zulässig sein. Dies gilt auch für Systeme, die in besonderen Fällen zu einer Leistungskontrolle der Beschäftigten erforderlich sind (etwa Wachpersonal).

Zu Absatz 12

In Anlehnung an § 26 Absatz 6 BDSG wird in Absatz 12 klargestellt, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

Begründung zu § 19 Verarbeitung zu künstlerischen oder literarischen Zwecken

Zu Absatz 1

Artikel 85 Absatz 1 DSGVO beauftragt die Mitgliedstaaten, durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß der DSGVO mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu literarischen Zwecken in Einklang zu bringen. Dafür gesteht Artikel 85 Absatz 2 DSGVO bestimmte Abweichungsbefugnisse vom Regelungsgehalt der Grundverordnung zu.

Die literarische Arbeit ist mit den Anforderungen der DSGVO nicht vollends in Einklang zu bringen. Die Verpflichtung zum Schutz des Rechts auf freie Meinungsäußerung erfordert es, Abweichungen zu regeln.

Zu Absatz 2

Im Anwendungsbereich der künstlerischen und literarischen Arbeit würde das Recht auf freie Meinungsäußerung leer laufen, wenn Berichtigungs- und Löschungsansprüche vollumfänglich zur Durchsetzung gelangten. So kommt eine Verpflichtung zur Berichtigung oder Löschung bereits veröffentlichter oder zur Veröffentlichung vorgesehener künstlerischer und literarischer Erzeugnisse gemäß den Vorgaben der DSGVO nicht ohne weiteres in Betracht. Das Recht

auf informationelle Selbstbestimmung vermittelt gleichwohl einen Anspruch des Betroffenen auf Gewährleistung von Vollständigkeit und Richtigkeit seiner Daten. Ein Ausgleich dieser Interessen wird dadurch mit der Verpflichtung zur parallelen Aufbewahrung und Übermittlung erzielt.
Die gebündelte Regelung für künstlerische und literarische Zwecke im DSG NRW ist zum einen dadurch bedingt, dass ein gleichartiges Regelungsbedürfnis für alle Konfliktlagen besteht und zum anderen, weil ein vorrangiges Anliegen des Datenschutzes umgesetzt wird.

Begründung zu § 20 Videoüberwachung

Die neue Regelung der Videoüberwachung für öffentliche Stellen findet ihre Grundlage in Artikel 6 Absatz 1 Buchstabe e) DSGVO. Durch die Verwendung des Begriffes „Verarbeitung“ im Zusammenhang mit der Videoüberwachung wird im Einklang mit der Definition in Artikel 4 Nr. 2 DSGVO verdeutlicht, dass sowohl die Beobachtung im Sinne eines Erhebens, als auch die Speicherung von personenbezogenen Daten gleichermaßen zulässig ist.
Da die Videoüberwachung, die regelmäßig mit einer Speicherung der Daten verbunden ist, bestimmt ist, um die Funktionsfähigkeit der betroffenen Behörden, Gerichte und der anderen öffentlichen Stellen zu gewährleisten, liegt sie im öffentlichen Interesse.

Zu Absatz 1

Die Videoüberwachung zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder Besitzes sowie zur Kontrolle von Zugangsberechtigen dient der Gewährleistung der Funktionsfähigkeit öffentlicher Stellen und damit mittelbar deren Aufgabenerfüllung, so dass die Videoüberwachung auch zu diesen Zwecken auf Artikel 6 Absatz 1 Buchstabe e DSGVO gestützt werden kann. Absatz 1 normiert zusätzlich zu dem sich aus Artikel 6 Absatz 1 Buchstabe e) DSGVO unmittelbar ergebenden Grundsatz der Erforderlichkeit der Verarbeitung, entsprechend der bisherigen Vorschrift (§ 29b Absatz 1 Satz 1 DSG NRW a.F.), dass keine Anhaltspunkte dafür bestehen dürfen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.
Vom Begriff der Videoüberwachung umfasst sind Verfahren der reinen Beobachtung ebenso wie die Speicherung der Überwachungsbilder. Der Begriff der Verarbeitung in Absatz 1 ist umfassend und bezieht sich auf alle Verarbeitungsschritte, die zur Erreichung des ursprünglichen Zwecks erforderlich sind.

Zu Absatz 2

Absatz 2 enthält wie bisher eine Regelung, die die Transparenz der Videoüberwachung gewährleistet. Aufgrund der Vorgaben in Artikel 13 Absätze 1 und 2 DSGVO ist es erforderlich, eine Regelung zu treffen, die eine diesen Vorgaben entsprechende Information der betroffenen Person gewährleistet. Dabei erscheint es sachgerecht, den Umstand der Videoüberwachung in Symbolform oder als Piktogramm darzustellen. Weiter sind der Name und die Kontaktdaten des Verantwortlichen, der Zweck der Verarbeitung sowie deren Rechtsgrundlage kenntlich zu machen. Die weiteren Pflichtinformationen gemäß Artikel 13 Absatz 2 Buchstabe a DSGVO sind ebenfalls am Ort der Videoüberwachung an einer für die betroffene Person zugänglichen Stelle zur Verfügung zu stellen, beispielsweise in Form eines Aushanges. „Frühestmöglich“ bezieht sich dabei im Sinne des Artikels 13 in der Regel auf den Zeitpunkt der Erhebung, soll aber gleichfalls Fallgestaltungen mitumfassen, in denen eine Kenntlichmachung bei Erhebung noch nicht möglich ist. In derlei Fällen ist die Mitteilung der in Absatz 2 gebotenen Informationen unverzüglich nachzuholen.

Zu Absatz 3

Absatz 3 regelt die Weiterverarbeitung der durch die Videoüberwachung erhaltenen Daten zu einem anderen Zweck. Diese Vorschrift ist Spezialnorm zu § 9 Absatz 2 des Gesetzes, indem die zulässigen Zweckänderungsgründe bei der Verarbeitung von Daten aus einer Videoüberwachung zum Schutz der Rechte der betroffenen Personen beschränkt werden. Die europarechtliche Regelungskompetenz ergibt sich aus Artikel 6 Absatz 4 i.V.m. Artikel 23 Absatz 1 Buchstaben c,d, i und j DSGVO. Die Regelung dient gleichermaßen dem Schutz der betroffenen Personen und den Rechten und Freiheiten Dritter. Neben der Beweissicherungsfunktion im Strafprozess kann die Videoüberwachung damit insbesondere der Durchsetzung zivilrechtlicher Ansprüche des Verantwortlichen und Dritter dienen.

Zu Absatz 4

Nach Artikel 17 Absatz 1 Buchstabe a der DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind. Diesem Grundsatz trägt Absatz 4 mit seiner Formulierung Rechnung. Mit Absatz 4 wird durch die Aufnahme einer Höchstspeicherfrist eine Regelung im Sinne des Artikels 6 Absatz 3 Satz 3 der DSGVO getroffen. Daneben wird für den Fall, dass die Daten für Zwecke der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von Rechtsansprüchen oder wegen entgegenstehender schutzwürdiger Interessen betroffener Personen weiterhin benötigt werden, eine auch über die Höchstspeicherfrist hinausgehende Speicherung zugelassen. Damit wird die eigentlich bestehende Löschungspflicht eingeschränkt. Dies ist nach Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 zulässig.

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

Begründung zu § 21 Anwendbarkeit der Verordnung (EU) 2016/679

Die in diesem Abschnitt geregelten besonderen Verarbeitungssituationen unterfallen gemäß Artikel 2 Absatz 2 DSGVO nicht dem Anwendungsbereich des Unionsrechts.
Nach der Auffangregelung des § 5 Absatz 6 dieses Gesetzes ist jedoch auch auf solche Verarbeitungssituationen das Unionsrecht entsprechend anwendbar, es sei denn, es wird durch dieses Gesetz oder durch andere spezielle Rechtsvorschriften etwas anderes geregelt. § 21 trifft für diesen Abschnitt eine solche besondere Regelung im DSG NRW. Soweit vereinzelte Rechtsvorschriften der DSGVO dennoch angewendet werden sollen, werden sie explizit in den Paragrafen benannt.

Begründung zu § 22 Öffentliche Auszeichnungen und Ehrungen

Mit § 22 werden die Voraussetzungen für die Zulässigkeit der Verarbeitung personenbezogener Daten zur Vorbereitung von Auszeichnungen und Ehrungen sowie im Hinblick auf besondere Kategorien personenbezogener Daten im Sinne des Artikel 9 Absatz 2 Buchstabe g DSGVO normiert.
Die Ordensverleihung ist ein außergerichtlicher Gunstbeweis, der sich ohne Begründungszwang und Überprüfbarkeit vollzieht. Von der vollumfänglichen Anwendbarkeit der DSGVO wird in diesen Fällen abgesehen, da ein besonderes öffentliches Interesse an einer tragfähigen Auswahlentscheidung besteht, welche auf einer vollumfängliche Würdigung aller Aspekt beruht und auch die persönliche Integrität der möglicherweise auszuzeichnenden oder zu ehrenden Person umfasst.

Zu Absatz 1

Absatz 1 regelt die Erhebungsbefugnis der vorbereitenden Stelle im Hinblick auf die zur Vorbereitung der Entscheidung erforderlichen Daten und bestimmt zum Schutz der Rechte der betroffenen Personen eine strenge Zweckbindung. Zur Vorbereitung der Entscheidung sind alle Daten erforderlich, die zur Beurteilung der Würdigkeit der betroffenen Person benötigt werden. Dies betrifft einerseits die Aspekte des der Auszeichnung zugrundliegenden Sachzusammenhangs. Andererseits kann aber auch die persönliche Integrität der auszuzeichnenden Person von Bedeutung sein, so dass je nach Einzelfall auch diesbezügliche Informationen erhoben werden dürfen.

Zu Absatz 2

Korrespondierend zu Absatz 1 regelt Absatz 2 eine Übermittlungsbefugnis auf Ersuchen bzw. Anforderung der für die Auszeichnung oder Ehrung zuständigen Stelle. Die Gewährleistung, dass nur sowohl in sachlicher als auch in persönlicher Hinsicht würdige Personen durch staatliche Stellen ausgezeichnet oder geehrt werden, ist ein wichtiges öffentliches Interesse, das durch die Norm sichergestellt werden soll.

Zu Absatz 3

Mit Absatz 3 wird normiert, dass eine Erhebung oder Übermittlung personenbezogener Daten dann nicht erfolgen darf, wenn die Person Auszeichnungen oder Ehrungen und/oder in diesem Zusammenhang stehende Datenverarbeitungen widersprochen hat.

Zu Absatz 4

Absatz 4 regelt in Anlehnung an § 21 dieses Gesetzes, welche Rechtsvorschriften der DSGVO im Zusammenhang mit der Entscheidung über öffentliche Auszeichnungen und Ehrungen entsprechend anzuwenden sind. Hierdurch wird sichergestellt, dass die Anforderungen der DSGVO in Bezug auf die Grundsätze der Verarbeitung und den technischen und organisatorischen Datenschutz eingehalten werden und die Datenverarbeitung der Kontrolle durch die und den Landesbeauftragten unterliegt. Somit kann auch in dieser besonderen Verarbeitungssituation außerhalb der DSGVO der notwendige Schutz der Daten der betroffenen Person gewährleistet werden. Die Vorschriften der DSGVO über die Informationspflicht (Artikel 13 und 14), das Auskunftsrecht (Artikel 15) und die Mitteilungspflicht (Artikel 19) sind nicht entsprechend anzuwenden.

Begründung zu § 23 Begnadigungsverfahren

§ 23 Absatz 1 Satz 1 des Gesetzes ist die allgemeine Befugnisnorm zur Datenverarbeitung in Gnadensachen. Auch der Rechtsbereich des Begnadigungsverfahrens unterliegt nicht dem Anwendungsbereich der DSGVO und ist insofern durch nationales Recht frei zu gestalten. Aufgrund der Besonderheit des Gnadenrechts unterliegt es nicht der Kontrolle durch die Landesbeauftragte für Datenschutz und Informationsfreiheit oder den Landesbeauftragten für den Datenschutz und Informationsfreiheit. § 23 Absatz 2 normiert gemäß § 21 dieses Gesetzes, welche Regelungen der DSGVO zur Anwendung kommen. Dies betrifft die Grundsätze der Verarbeitung personenbezogener Daten sowie den Bereich des technischen und organisatorischen Datenschutzes. Die Rechte der betroffenen Personen ergeben sich aus der Gnadenordnung unmittelbar. Damit kann auch in dieser besonderen Verarbeitungssituation außerhalb der DSGVO der notwendige Schutz der Daten der betroffenen Person gewährleistet werden.

Kapitel 4 Pflichten des Verantwortlichen

Begründung zu § 24 Datenschutz-Folgenabschätzung

Zu Absatz 1 und 2

Absatz 1 konkretisiert das dem Landesgesetzgeber nach Artikel 35 Absatz 1 Satz 2 DSGVO eingeräumte Ermessen dahingehend, dass bei der Einführung neuer Verarbeitungsvorgänge eine (erneute) Datenschutz-Folgenabschätzung durch die jeweilige öffentliche Stelle nicht durchgeführt werden soll, sofern eine solche Überprüfung bereits durch die oberste Landesbehörde für wesensgleiche Verfahren durchgeführt wurde. „Im Wesentlichen“ bezieht sich dabei auf Fallkonstellationen, in denen die jeweilige öffentliche Stelle sich nur Teile eines insgesamt von der sachlich zuständigen obersten Landesbehörde vorab geprüften (Fach-) Verfahrens zu Nutze macht. Die Ergebnisse bereits durchgeführter Datenschutz-Folgenabschätzungen kann den öffentlichen Stellen in dem jeweiligen Geschäftsbereich zur Verfügung gestellt werden, soweit dadurch keine Gefährdung der Sicherheit der von der Datenschutz-Folgenabschätzung betroffenen IT- Systeme besteht.

Zu Absatz 3

Absatz 3 bezieht die Regelung des Absatzes 1 auch auf weitere öffentliche Stellen. Durch die Möglichkeit der Übernahme von Verfahren sollen die Behörden und öffentlichen Stellen entlastet und ein ökonomisches Arbeiten gewährleistet werden. Dies ergibt sich auch aus Erwägungsgrund 92, der ausführt, dass in einem solchen Fall die Datenschutzfolgeabschätzung von vornherein nicht auf ein bestimmtes Projekt zu beziehen ist, sondern thematisch breiter angelegt werden soll.

Kapitel 5 Landesbeauftragter für Datenschutz und Informationsfreiheit

Kapitel VI passt die Regelungen des DSG NRW a. F. zu der oder dem Landesbeauftragten für den Datenschutz und Informationssicherheit und deren oder dessen Befugnisse an die Vorgaben der DSGVO an. Damit wird an die Umsetzungsschritte zur Wahrung der „völligen Unabhängigkeit“, wie sie im „Gesetz über die Unabhängigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit“ aus dem Jahre 2011 vollzogen worden sind, angeknüpft. Zugleich werden die Vorgaben der DS-RL umgesetzt.
Unter Beibehaltung der bisherigen Regelungen wird das Amt der oder des Landesbeauftragten als Aufsichtsbehörde im Sinne des Artikels 51 DSGVO als selbständige Landesbehörde errichtet.
Mit der Beibehaltung einer selbständigen und weisungsfreien Aufsichtsbehörde wird den Vorgaben der DSGVO Rechnung getragen, eine Aufsichtsbehörde zu errichten, die den Anforderungen gemäß Artikel 52 Absatz 1 DSGVO entspricht. d. h. sie kann ihre Aufgaben in völliger Unabhängigkeit wahrnehmen. Zur Gewährleistung dieser Unabhängigkeit erfolgen entsprechend den Vorgaben der DSGVO flankierende Regelungen insbesondere in Bezug auf die Wahl, Ernennung und die Amtszeit, einschließlich der sich daraus ergebenden Aufgaben und Befugnisse der oder des Landesbeauftragten.

Begründung zu § 25 Errichtung und Rechtsstellung

Zu Absatz 1

Absatz 1 legt in Anlehnung an § 21 Absatz 1 DSG NRW a. F. in Satz 1 zunächst die Funktion der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit als Aufsichtsbehörde im Sinne des Artikel 51 DSGVO fest. Satz 2 regelt das Verfahren der Wahl und Ernennung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit. Nach Artikel 53 Absatz 1 DSGVO sehen die Mitgliedstaaten ein transparentes Ernennungsverfahren durch das Parlament, die Regierung, das Staatsoberhaupt oder eine unabhängige Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird, vor. Zudem wird in Absatz 1 in Durchführung des Artikels 53 Absatz 2, 54 Absatz 1 Buchstabe b DSGVO die Anforderungen an die Qualifikation der oder des Landesbeauftragten unter Berücksichtigung der laufbahnrechtlichen Neuerungen des Dienstrechtsmodernisierungsgesetzes geregelt.

Zu Absatz 2

Absatz 2 unterstreicht die bereits in Artikel 77a Absatz 1 Landesverfassung Nordrhein-Westfalen verankerte Stellung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit als nach Artikel 52 DSGVO völlig unabhängige Aufsichtsbehörde. Gleichermaßen unterliegen die Bediensteten nur den Weisungen der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit.

Zu Absatz 3

Die in Absatz 3 getroffenen Regelungen zur Länge der Amtszeit und zur einmaligen Wiederwahl entsprechen den Vorgaben des Artikels 54 Absatz 1 Buchstabe d und e DSGVO. Die Begrenzung auf eine einmalige Wiederwahl berücksichtigt zum einen, dass angesichts der hohen Anforderungen hinsichtlich der Qualifikation und der fachlichen Erfahrung, die bei der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorausgesetzt wird, in aller Regel lebensältere Bewerber in Betracht kommen, die nicht selten während einer bzw. spätestens nach einer weiteren Amtsperiode den Ruhestand erreichen. Zum anderen stellt der Zeitraum von 16 Jahren als Höchstdauer der Amtszeit einen in jeder Hinsicht ausreichenden Gestaltungszeitraum für den Amtsinhaber dar. Nach Ablauf dieses langen Zeitraumes bietet die Neubesetzung des Amtes eine Chance, dieses Amt mit neuen Ideen und Vorstellungen zu führen. Satz 3 regelt die bislang in § 21 Absatz 2 Satz 2 DSG NRW a. F. vorgesehene Pflicht der oder des Landesbeauftragten zur Weiterführung des Amtes bis zur Ernennung einer Nachfolgerin oder eines Nachfolgers.
Absatz 3 regelt zugleich die Stellvertretung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit. Die Mitgliedstaaten haben zudem die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde zu schaffen. Die Wahrnehmung der Rechte der oder des Landesbeauftragten durch die Stellvertretung ist eine zweckmäßige, im engen Zusammenhang zu den Regelungsaufträgen des Artikel 54 Absatz 1 Buchstabe a und d DSGVO stehende Regelung zur Gewährleistung der Funktionsfähigkeit und Aufgabenerfüllung bei Abwesenheit der oder des Landesbeauftragten.

Zu Absatz 4

Für die beamtenrechtliche Angelegenheiten der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit in Person bestimmt Absatz 4 die zuständige Stelle, lässt dabei aber seine Unabhängigkeit unangetastet.

Zu Absatz 5

Absatz 5 regelt den Beginn und das Ende der Amtszeit der oder des Landesbeauftragten. Die Regelung entspricht den Vorgaben der Artikel 53 Absätze 3 und 4, 54 Absatz 1 Buchstabe c, d und f DSGVO und konkretisiert diese. Unter Berücksichtigung des Artikels 53 Absatz 4 DSGVO ist eine Amtsenthebung künftig nur nach Feststellung einer schweren Verfehlung durch die Richterdienstgerichte zulässig. Disziplinarische Maßnahmen unterhalb dieser Schwelle der schweren Verfehlung sind nach der Datenschutzgrundverordnung nicht möglich.

Zu Absatz 6

Die Regelung dient der Umsetzung von Artikel 52 Absätze 4 und 6 DSGVO. Durch die Beibehaltung der bisherigen Regelung in § 21 Absatz 4 DSG NRW a.F. wird der Haushalt der oder des Landesbeauftragen auch künftig im Einzelplan des Landtages in einem eigenen Kapitel ausgewiesen. Dies dient der Gewährleistung der Unabhängigkeit der oder des Landesbeauftragten.
Zur weiteren Stärkung der Unabhängigkeit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit auch in finanzieller Hinsicht normiert Satz 2 die entsprechende Anwendung der § 28 Absatz 3 und § 29 Absatz 3 LHO für die oder den Landesbeauftragten. Damit kann zukünftig nur der Haushaltsgesetzgeber über die finanzielle Ausstattung der oder des Landesbeauftragten entscheiden und nicht auch noch die Exekutive. Wie bei dem Präsidenten des Landtags und des Landesrechnungshofs sind bei der Haushaltsaufstellung die Abweichungen von den Vorschlägen und Unterlagen der oder des Landesbeauftragten der Landesregierung mitzuteilen bzw. der Vorschlag, über den kein Einvernehmen erzielt worden ist, ist unverändert dem Entwurf des Haushaltsplans beizufügen.
Mit dem (klarstellenden) Satz 3 wird gemäß Artikel 52 Absatz 6 DSGVO die Vorgabe erfüllt, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt.

Zu Absatz 7

Absatz 7 regelt die Modalitäten der autonomen Personalverwaltung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit. In Übereinstimmung mit § 21 Absatz 5 Sätze 2 und 3 DSG NRW a.F. bleibt die Personalrotation in der Landesverwaltung möglich. Auch besteht weiterhin die Möglichkeit zum Abschluss einer Verwaltungsvereinbarung mit dem für Inneres zuständigen Ministerium bezogen auf die Personalgewinnung und die Personalverwaltung.

Zu Absatz 8

Als Ausfluss aus Artikel 77a Absatz 2 Satz 2 Landesverfassung Nordrhein-Westfalen soll § 25 Absatz 8 die besondere Bindung zwischen der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit und dem Parlament verdeutlichen. Sie oder er kann sich jederzeit beispielsweise mit datenschutzrechtlichen Hinweisen oder bei unausräumbaren Meinungsverschiedenheiten mit der Landesregierung an den Landtag wenden. Ein Rederecht vor dem Landtag erwächst aus Absatz 8 allerdings nicht.

Begründung zu § 26 Zuständigkeit

§ 26 macht deutlich, dass die Funktion der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit über die Funktion nach Artikel 51 und 57 DSGVO hinaus reicht. Sie oder er überwacht ferner die Einhaltung der Bestimmungen dieses Gesetzes und ist zugleich Aufsichtsbehörde im Lande Nordrhein-Westfalen nach dem Bundesdatenschutzgesetz.

Begründung zu § 27 Aufgaben

Die Artikel 57 und 58 DSGVO regeln Aufgaben und Befugnisse der Aufsichtsbehörden. Sie eröffnen gleichzeitig Präzisierungs- und Regelungsoptionen im mitgliedstaatlichen Recht, von denen in § 27 Gebrauch gemacht wird.

In Absatz 1 ist in Anlehnung an § 22 Absatz 1 DSG NRW a. F. die Aufgabe zur Beratung und zur Information gegenüber öffentlichen Stellen beibehalten worden.

Absatz 2 verpflichtet die öffentlichen Stellen die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit bei ihren oder seinen Aufgaben ggf. durch Amtshilfe zu unterstützen.

Satz 3 entspricht § 22 Absatz 2 Satz 2 DSG NRW a.F.
Der Absatz 3 stellt eine Ausnahme bzw. Einschränkung zu Absatz 2 dar, soweit es sich um öffentliche Stellen im Sinne des § 203 Absatz 1 und 3 sowie Absatz 4 Satz 1 des Strafgesetzbuches handelt. Geschützt sind hierbei die in dieser Vorschrift genannten Personen oder deren Auftragsverarbeiter. Vom Regelungsumfang umfasst sind beispielsweise Notarinnen und Notare als Organe der Rechtspflege, die durch Hoheitsakt bestellt werden und der Dienstaufsicht der Landesjustizverwaltung unterliegen. Sie sind öffentliche Stellen der Länder im Sinne des Datenschutzgesetzes NRW. Mit der Regelung des Absatzes 3 wird die notarielle Verschwiegenheitspflicht geschützt. Ohne eine Einschränkung der Befugnisse der Aufsichtsbehörde käme es zu einer Kollision mit Pflichten des Geheimnisträgers. Die Regelung des Absatzes 3 ist dem § 29 Absatz 3 Bundesdatenschutzgesetz (neu) nachgebildet. Die Änderung ist sachgerecht und schützt das Recht auf informationelle Selbstbestimmung angemessen, indem sie die Einschränkung der Befugnisse der Aufsichtsbehörde auf das Geheimhaltungsinteresse der Betroffenen begrenzt.

In besonders gelagerten Fällen nach Absatz 4 kann es dazu führen, dass die Aufgabenwahrnehmung zur persönlichen Angelegenheit der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit als Behördenleiterin oder Behördenleiter, oder - im Falle ihrer oder seiner Verhinderung - von deren oder dessen Stellvertreter wird.

Absatz 5 entspricht § 22 Absatz 3 DSG NRW a.F.
Absatz 5 dient der Konkretisierung und Spezifizierung von Artikel 36 Absatz 4 DSGVO. Es soll bei Planungen zur Entwicklung, zum Aufbau oder zur wesentlichen Veränderung automatisierter Datenverarbeitungs- und Informationssysteme und Entwürfen für Rechts- oder Verwaltungsvorschriften sichergestellt werden, dass die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit frühzeitig unterrichtet wird, so dass eine Stellungnahme in dem jeweiligen Verfahren noch Berücksichtigung finden kann.

Begründung zu § 28 Befugnisse

Nach Artikel 58 Absatz 6 DSGVO kann jeder Mitgliedstaat vorsehen, dass die Aufsichtsbehörde neben den in Artikel 58 Absätze 1, 2 und 3 DSGVO vorgesehenen Befugnissen über zusätzliche Befugnisse verfügt. Von dieser Regelungsbefugnis wird dergestalt Gebrauch gemacht, dass die Aufsichtsbehörde vor der Wahrnehmung der Befugnisse nach Artikel 58 Absätze 1 bis 3 DSGVO die Möglichkeit - nicht aber die Verpflichtung - hat, ein formelles Beanstandungsverfahren durchzuführen. Hierzu werden die bisherigen Regelungen des § 24 DSG NRW a. F. aufgegriffen und modifiziert.

Zu Absatz 1

Absatz 1 enthält eine Privilegierung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit, weil sie oder er bei einer Datenerhebung im Rahmen einer Kontrollmaßnahme von einer Benachrichtigung des Betroffenen nach pflichtgemäßem Ermessen absehen kann.

Zu Absatz 2

Die Durchführung eines vorgeschalteten Beanstandungsverfahrens eröffnet in Absatz 2 die Möglichkeit, dass festgestellte Verstöße gegen die Vorschriften des Datenschutzes der jeweils zuständigen Rechts- oder Fachaufsichtsbehörde mitgeteilt werden und diese vor der etwaigen Ausübung der Befugnisse nach Artikel 58 Absatz 2 DSGVO unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhalten. Durch die Mitteilung wird insbesondere gewährleistet, dass die zuständige Fachaufsichtsbehörde Kenntnis von dem Verstoß erhält und vor der Ausübung weitergehender Befugnisse durch die oder den Landesbeauftragte(n) rechtliches Gehör findet. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und der Rechts- oder Fachaufsicht wird hierdurch reduziert. Widersprüchliche Auffassungen der Datenschutzaufsicht und der Fachaufsicht sind ggf. auf dem Gerichtsweg zu klären.

Zu Absatz 3

Absatz 3 enthält unter Beibehaltung der bisherigen Rechtslage (§ 24 Absatz 4 DSG NRW a.F.) Verfahrensregelungen.

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

Artikel 77 DSGVO regelt das Beschwerderecht. Durch § 29 wird dieses Recht weiter konkretisiert. Satz 2 stellt in Anlehnung an § 25 Absatz 2 DSG NRW a.F. klar, dass niemand benachteiligt werden darf, weil er sein Beschwerderecht ausgeübt hat.
Satz 3 regelt in Anlehnung an § 25 Absatz 1 DSG NRW a.F., dass bei einer Beschwerde der Dienstweg nicht eingehalten werden muss. So soll verhindert werden, dass eine begründete Beschwerde auf dem Dienstweg gestoppt wird.
Durch diesen Paragrafen soll die Effektivität des Beschwerderechts abgesichert werden, indem der Betroffene keine Repressionen oder Ähnliches zu fürchten hat.

Begründung zu § 30 Tätigkeitsbericht, Gutachtertätigkeit

Die Pflicht der Aufsichtsbehörde, jährlich einen Tätigkeitsbericht zu erstellen und diesen zugänglich zu machen, ergibt sich aus Artikel 59 DSGVO unmittelbar. Die DSGVO enthält zwar keine Pflicht der Landesregierung, zu diesem Bericht eine Stellungnahme abzugeben. Gleichwohl soll an dem bisherigen Verfahren und der Diskussion des Berichts im Landtag festgehalten werden. Deshalb wird entsprechend dem bisherigen Recht (§ 27 Absatz 1 DSG NRW a.F.) in Absatz 1 geregelt, dass die Landesregierung zu diesem Bericht eine Stellungnahme abzugeben hat, soweit ihr Verantwortungsbereich betroffen ist. Im Übrigen trägt Satz 1 § 13 Absatz 3 IFG NRW Rechnung. Indem es der Aufsichtsbehörde anheimgestellt ist, den Jahresbericht nach Artikel 59 DSGVO in jedem zweiten Jahr mit dem 2-Jahres-Bericht über ihre oder seine Tätigkeit als Beauftragte oder Beauftragter für das Recht auf Information zu verbinden oder nicht.

Das bisherige Recht des Landtages, die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit mit der Erstattung von Gutachten in Datenschutzfragen zu betrauen (§ 27 Absatz 2 DSG NRW a. F), bleibt in Absatz 2 in Einklang mit Artikel 57 Absatz 1 Buchstabe c) DSGVO bestehen.

Kapitel 6 Behördlicher Datenschutzbeauftragter

Begründung zu § 31 Geheimhaltung, Zeugnisverweigerungsrecht und Abberufung

§ 31 enthält konkretisierende Regelungen zu den Vorgaben zum behördlichen Datenschutzbeauftragten gemäß Artikel 37 ff. DSGVO. In teilweiser Anlehnung an § 32a DSG NRW a. F. werden Aspekte der Verschwiegenheitspflicht, des Zeugnisverweigerungsrechts und des Benachteiligungsverbots in § 31 einer Regelung bzw. einer Konkretisierung zugeführt.

Zu Absatz 1

Übernimmt die Möglichkeit aus § 32 a Absatz 1 Satz 2 DSG NRW a. F. gegebenenfalls mehrere behördliche Datenschutzbeauftragte sowie Vertreter zu bestellen. Allerdings kann dies nur gelten, sofern den Datenschutzbeauftragten voneinander klar abgegrenzte Verantwortungs- und Aufgabenbereiche zugeteilt werden.

Zu Absatz 2

Ausgehend von Artikel 38 Absatz 4 DSGVO, nach der betroffene Personen den behördlichen Datenschutzbeauftragten zu Rate ziehen können, wird eine Verschwiegenheitspflicht des behördlichen Datenschutzbeauftragten in Anlehnung an § 32a Absatz 4 Satz 2 DSG a. F. geregelt.

Zu Absatz 3

Absatz 3 enthält eine Regelung zum Zeugnisverweigerungsrecht, die dem § 6 Absatz 6 BDSG (neu) nachgebildet ist. Dabei ist zu beachten, dass der Bund im Rahmen seiner Gesetzgebungskompetenz nur Regelungen für die oder den Datenschutzbeauftragten von Bundesbehörden getroffen hat. Die Regelung in Absatz 3 ist daher erforderlich, um eine kohärente Rechtsstellung der oder des Datenschutzbeauftragten in der Landesverwaltung zu erzielen.

Die Regelungskompetenz lässt sich für die Absätze 1 bis 3 aus Artikel 38 Absatz 5 DSGVO folgern, weil hierdurch Regelungen zum behördlichen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit getroffen werden.

Zu Absatz 4

Bei dem besonderen Abberufungs- und Kündigungsschutz der oder des behördlichen Datenschutzbeauftragten in Absatz 3 handelt es sich um eine arbeitsrechtliche Regelung, die ergänzend zu den Vorgaben der Verordnung (EU) 2016/679 (hier: Benachteiligungsverbot nach Artikel 38 Absatz 3 Satz 2 DSGVO) bestehen darf.

Kapitel 7 Straf- und Bußgeldvorschriften

Begründung zu § 32 Geldbußen

Nach dieser Vorschrift dürfen gegen öffentliche Stellen im Sinne des § 5 Absatz 4 Geldbußen nach Artikel 83 DSGVO verhängt werden. Damit legt § 32 gleichzeitig fest, dass solche Geldbußen gegen öffentliche Stellen nach § 5 Absatz 1 gerade nicht verhängt werden dürfen.

Die Befugnis zu dieser Regelung ergibt sich aus Artikel 83 Absatz 7 DSGVO. Danach kann jeder Mitgliedstaat festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

Sanktionen in der von Artikel 83 DSGVO vorgesehenen Form und Höhe sind in dem öffentlichen Bereich weder erforderlich noch angemessen und dem deutschen Verfassungsrecht fremd. Bei Verstößen gegen die in Artikel 83 Absatz 1 bis 6 DSGVO genannten Bestimmungen sind vielmehr die Rechtsaufsichtsbehörden zum Handeln aufgerufen.

Begründung zu § 33 Ordnungswidrigkeiten

Zu den Absätzen 1 und 2

In Artikel 83 DSGVO sind die Bedingungen und Tatbestände lediglich für die Verhängung von Geldbußen gegen verantwortliche Stellen und Auftragsverarbeiter geregelt. Die DSGVO enthält keine Regelungen zur Verhängung von Geldbußen gegenüber Mitarbeitern der verantwortlichen Stelle. Artikel 84 Absatz 1 DSGVO enthält diesbezüglich eine Öffnungsklausel. Danach legen die Mitgliedstaaten „insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen“, Vorschriften über Sanktionen fest.
§ 33 Absatz 1 greift auf der Grundlage dieser Öffnungsklausel die bisherige Rechtslage auf, nach der die Verhängung von Geldbußen auch gegen die bei der Datenverarbeitung beschäftigten Personen möglich war. Geahndet wird in Verbindung mit § 2 und § 10 des Gesetzes über Ordnungswidrigkeiten(OWiG) nur vorsätzliches Verhalten von Beschäftigten. § 33 Absatz 2 begrenzt die Höhe des Bußgeldes wie bisher auf 50.000 €.

Zu Absatz 3

In Abkehr von der Regelung des § 34 DSG NRW a.F. ist künftig die oder der Landesbeauftragte für Datenschutz und Informationssicherheit sachlich allein zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 OwiG für die Verfolgung von Ordnungswidrigkeiten nach § 33 DSG NRW.

Zu Absatz 4

Mit Absatz 4 wird von der Öffnungsklausel des Artikels 83 Absatz 7 DSGVO Gebrauch gemacht, national zu regeln, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen verhängt werden können. Auch Geldbußen nach § 33 sollen nicht gegen öffentliche Stellen nach § 5 Absatz 1 verhängt werden dürfen.

Der Bußgeldrahmen in § 33 DSG NRW ist als Sanktion gemäß Artikel 84 Absatz 1 Satz 2 DSGVO wirksam, verhältnismäßig und abschreckend.

Begründung zu § 34 Straftaten

Artikel 84 Absatz 1 DGVO berechtigt und verpflichtet die Mitgliedstaaten, „andere Sanktionen“ für Verstöße gegen die Verordnung festzulegen. Artikel 84 DSGVO ist damit insbesondere eine Öffnungsklausel, um neben Geldbußen im Sinne des Artikels 83 DSGVO mitgliedstaatlich strafrechtliche Sanktionen vorzusehen. Hiervon wird mit § 34 unter weitgehender Beibehaltung der bisherigen Regelungen Gebrauch gemacht.

Absatz 2 enthält nunmehr ein Antragserfordernis. Der erforderliche Strafantrag kann auch von der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit gestellt werden.

Absatz 3 enthält wie § 33 Absatz 2 DSG NRW a.F. eine Subsidiaritätsklausel, weil sich der Regelungsgehalt der Vorschrift mit § 203 Absatz 2 Strafgesetzbuch überschneiden kann. Das Bundesrecht hat in einem solchen Fall Vorrang.

Der Strafrahmen in § 34 DSG NRW ist als Sanktion gemäß Artikel 84 Absatz 1 Satz 2 DSGVO wirksam, verhältnismäßig und abschreckend.

Teil 3 Umsetzung der Richtlinie (EU) 2016/680

Kapitel 1 Allgemeine Bestimmungen

Der Zweite Teil dieses Gesetzes dient der Umsetzung der Richtlinie (EU) 2016/680. Ergänzend dazu werden bereichsspezifische Regelungen im jeweiligen Fachrecht geregelt.

Begründung zu § 35 Anwendungsbereich

§ 35 regelt den Anwendungsbereich des dritten Teils. Er gilt nur für die Verarbeitung durch öffentliche Stellen, 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 sind. Erfasst sind hiervon insbesondere die Polizeibehörden und die Justizbehörden.

Hervorzuheben ist, dass der Begriff der Strafvollstreckung in Satz 1 auch den Straf- und Maßregelvollzug einbezieht. Der Begriff der Strafvollstreckung bezieht sich auf die Strafvollstreckung im weiteren Sinne. Diese ist gleichbedeutend mit dem Begriff der Strafverwirklichung, die neben der Strafvollstreckung im engeren Sinne auch den Straf- und Maßregelvollzug umfasst.

Aufgabe der Finanzämter für Steuerstrafsachen und Steuerfahndung ist die Ermittlung, Aufdeckung, Verfolgung und Ahndung von Steuerstraftaten und –ordnungswidrigkeiten. In selbständigen Ermittlungsverfahren stehen ihnen die Rechte und Pflichten der Staatsanwaltschaft zu, § 399 AO. Die mit der Steuerfahndung betrauten Dienststellen haben im Strafverfahren wegen Steuerstraftaten dieselben Rechte und Pflichten wie die des Polizeivollzugsdienstes nach den Vorschriften der Strafprozessordnung.

Die Finanzverwaltung fällt daher – soweit sie mit der Verfolgung von Steuerstraftaten betraut ist – in den Regelungsbereich der Richtlinie (EU) 2016/680. Entsprechend ist der diese Richtlinie umsetzende Teil 3 des DSG NRW auch für die Finanzverwaltung anwendbar. Die Anwendbarkeit wird durch die explizite Aufnahme der Finanzverwaltung in die Aufzählung des § 35 Absatz 1 DSG NRW sichergestellt.

Gemäß Absatz 2 unterfällt bei den Ordnungsbehörden das Handeln der DS-RL, wenn sie mit der Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten befasst sind. Dies ergibt sich aus Erwägungsgründen 11-13 der DS-RL. Erwägungsgrund 11 DS-RL konkretisiert die Art der zuständigen Behörden dahingehend, dass nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden erfasst sind, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedsstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke der Richtlinie übertragen wurden. Dies schließt die Ordnungsbehörden bei der Durchführung von Ordnungswidrigkeitenverfahren ein. Erwägungsgrund 12 DS-RL stellt klar, dass die Aufrechterhaltung der öffentlichen Ordnung als Aufgabengruppe ebenso im Geltungsbereich der Richtlinie anzusiedeln ist.
Aus Erwägungsgrund 13 DS-RL ergibt sich, dass der Richtlinien-Begriff der „Straftat“ ein eigenständiger Begriff des Unionsrechts ist. Damit umfasst er auch Ordnungswidrigkeiten nach deutschem Recht, da dem Unionsrecht und vielen Mitgliedsstaaten die deutsche Trennung zwischen dem Straf- und Ordnungsrecht fremd ist.
Ebenfalls erstreckt sich dieser Teil und die DS-RL gem. § 36 Nummer 8 b auch auf Beliehene.
Vom Anwendungsbereich der DS-RL nicht erfasst sind insbesondere reine Verwaltungsangelegenheiten der Polizei- und Justizbehörden, für diese gilt die DSGVO sowie der Erste und Zweite Teil dieses Gesetzes.
Als Organe der Rechtspflege werden Staatsanwaltschaften und Strafgerichte bei der Datenverarbeitung auf die Regelungen des BDSG verwiesen, da dieses gem. § 1 Absatz 1 Nummer 2 b) BDSG auch auf öffentliche Stellen der Länder anzuwenden ist, soweit sie als Organe der Rechtspflege tätig werden und es sich bei ihrer Tätigkeit nicht um Verwaltungsangelegenheiten handelt.

Absatz 3 entspricht § 5 Absatz 5 dieses Gesetzes. Sofern die Verarbeitung personenbezogener Daten im bereichsspezifischen Landesrecht im Anwendungsbereich der DS-RL gesondert geregelt ist, sind diese Vorschriften wie bisher vorrangig anzuwenden.

Begründung zu § 36 Begriffsbestimmungen

§ 36 ähnelt § 3 DSG-NRW a.F. und bestimmt die notwendigen Legaldefinitionen für den Anwendungsbereich der DS-RL. Dabei wurden die Definitionen im Wesentlichen aus Artikel 3 DS-RL übernommen.

Kapitel 2 Grundsätze

Begründung zu § 37 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 37 dient der Umsetzung von Artikel 4 Absatz 1 DS-RL und entspricht im wesentlichen Artikel 5 Absatz 1 DSGVO. Er normiert die generellen Verarbeitungsgrundsätze im Anwendungsbereich dieses Teils.

Begründung zu § 38 Einwilligung

In § 38 finden sich die Voraussetzungen für eine wirksame Einwilligung. Als Grundlage dient § 51 BDSG welcher Elemente aus Artikel 7 der Verordnung (EU) 2016/679 übernommen hat. Absatz 1 entspricht Artikel 7 Absatz 1, Absatz 2 Artikel 7 Absatz 2 und Absatz 3 Artikel 7 Absatz 3 der Verordnung (EU) 2016/679.

Begründung zu § 39 Verarbeitung zu einem anderen Zweck als dem Erhebungszweck

In § 39 wird Artikel 4 Absatz 2 DS-RL umgesetzt. Satz 1 regelt, dass Daten zu einem anderen als dem ursprünglichen Zweck verarbeitet werden dürfen, soweit auch dieser Zweck unter den Anwendungsbereich der DS-RL bzw. dieses Teils des Gesetzes fällt. Zusätzliche Anforderungen an die Zweckänderung innerhalb der in § 36 genannten Zwecke aufgrund nationalen Verfassungsrechts (so etwa der Grundsatz der hypothetischen Datenneuerhebung, vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06) werden in den Fachgesetzen, wie dem Polizeigesetz NRW, umgesetzt.
Satz 2 erweitert die Möglichkeit der Verarbeitung auch auf einen Zweck außerhalb des Regelungsbereiches dieses Teils, soweit dies durch eine Rechtsvorschrift zugelassen wird.

Begründung zu § 40 Verarbeitung wissenschaftlichen oder statistischen Zwecken

Durch § 40 soll Artikel 4 Absatz 3 DS-RL umgesetzt werden. Demnach dürfen Daten auch zu wissenschaftlichen, statistischen oder historischen Zwecken verarbeitet werden, soweit diese Verarbeitung unter die in § 35 genannten Zwecke gefasst werden kann.
Voraussetzung hierfür ist, dass geeignete Vorkehrungen zugunsten der Rechtsgüter der betroffenen Person getroffen werden; dazu zählen insbesondere die Anonymisierung von Daten (die gemessen am jeweiligen Forschungszweck so zeitnah wie möglich zu erfolgen hat) oder die räumliche und organisatorische Abtrennung der Forschung betreibenden Stellen. Die Vorkehrungen sind im bereichsspezifischen Recht weiter auszudifferenzieren.

Begründung zu § 41 Datengeheimnis

Dieser Paragraph entspricht dem § 6 DSG NRW a.F. und soll die Einhaltung des Datenschutzes auch unmittelbar durch die mit der Datenverarbeitung beschäftigten Personen gewährleisten.

Begründung zu § 42 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

§ 42 dient der Umsetzung von Artikel 6 DS-RL. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung werden dem bereichsspezifischen Recht überlassen.

Begründung zu § 43 Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

§ 43 dient der Umsetzung von Artikel 7 Absatz 1 DS-RL. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung werden dem bereichsspezifischen Recht überlassen.

Begründung zu § 44 Verfahren bei Übermittlung

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 DS-RL. Ferner ist bei der Anwendung und Auslegung der Anforderungen des § 44 zu beachten, dass sich die Frage nach der „Aktualität“ von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen“ Daten zu übermitteln bzw. bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten wie alte Meldeadressen, alte (Geburtsnamen) etc. bedeutsam und für die Aufgabenerfüllung erforderlich sein.

Zu Absatz 2

Absatz 2 setzt Artikel 9 Absatz 3 DS-RL um. Beispiele für die im Fachrecht vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Zu Absatz 3

Absatz 3 setzt Artikel 9 Absatz 4 DS-RL um.

Begründung zu § 45 Verarbeitung besonderer Kategorien personenbezogener Daten

Die Vorschrift dient der Umsetzung von Artikel 10 DS-RL.

Zu Absatz 1

Absatz 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Unbedingt erforderlich sein kann die Aufgabenerfüllung insbesondere zur Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person (Artikel 10 Buchstabe b DS-RL) oder wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat (Artikel 10 Buchstabe c DS-RL).

Zu Absatz 2

In Absatz 2 wird in Satz 1 klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen beachtet werden müssen. In Satz 2 wird auf mögliche Maßnahmen zur Umsetzung dieser Vorgabe, wie sie in § 15 dieses Gesetzes aufgelistet sind, Bezug genommen. Die genaue Wahl der geeigneten Garantien hat im bereichsspezifischen Recht zu erfolgen.

Begründung zu § 46 Automatisierte Einzelentscheidungen

§ 46 setzt Artikel 11 DS-RL um.

Zu Absatz 1

Das Verbot der automatischen Einzelentscheidung bezieht sich dabei jedoch nur auf Fälle, in denen die Entscheidung nachteilig für die betroffene Person ist oder sie erheblich beeinträchtigt. Eine Ausnahme besteht insoweit wenn eine Rechtsvorschrift dies ausdrücklich zulässt.

Zu Absatz 2

Absatz 2 trifft eine Sonderregelung für besondere Kategorien personenbezogener Daten i.S.d. § 36 Nummer 18.

Zu Absatz 3

Dieser Absatz dient der Umsetzung von Artikel 11 Absatz 3 DS-RL und gewährleistet den bedeutenden Schutz besonderer Kategorien personenbezogener Daten von natürlichen Personen.

Kapitel 3 Rechte der betroffenen Personen

Begründung zu § 47 Allgemeine Informationen zu Datenverarbeitungen

Die Vorschrift dient der Umsetzung von Artikel 13 Absatz 1 DS-RL. Dadurch sollen aktive Informationspflichten des Verantwortlichen sichergestellt werden. Dieser Informationspflicht sollen Verantwortliche in allgemeiner Form nachkommen können. Aus Erwägungsgrund 42 DS-RL ergibt sich dazu die Möglichkeit der Information über die Website des Verantwortlichen. Sinn und Zweck dieser Regelung ist, dass betroffene Personen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können sollen und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte bekommen.

Begründung zu § 48 Benachrichtigung betroffener Personen

§ 48 betrifft Fälle, in denen in bereichsspezifischen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in Artikel 13 Absatz 2 DS-RL bezeichneten „besonderen Fälle“ ist nicht verallgemeinernd auf Ebene des allgemeinen Datenschutzrechts möglich und muss somit im bereichsspezifischen Recht geleistet werden.

Zu Absatz 1

Absatz 1 stellt klar, welche Informationen betroffenen Personen von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen und dient dabei der Umsetzung von Artikel 13 Absatz 2 DS-RL.

Zu Absatz 2

Absatz 2 ermöglicht eine Einschränkung bzw. ein Aufschieben der in Absatz 1 genannten Benachrichtigungspflicht in den Fällen der Nummern 1 bis 5. § 48 Absatz 2 setzt damit Artikel 13 Absatz 3 DS-RL um. Im Einzelnen entspricht
Nummer 1 Artikel 13 Absatz 3 Buchstabe b
Nummer 2 Artikel 13 Absatz 3 Buchstabe c
Nummer 3 Artikel 13 Absatz 3 Buchstabe e
Nummer 4 Artikel 13 Absatz 3 Buchstabe d
Nummer 5 Artikel 13 Absatz 3 Buchstabe a

Den auf Artikel 13 Absatz 3 Buchstabe a bis e DS-RL fußenden Ausnahmen ist der Gedanke gemein, dass die Benachrichtigung nicht zur Beeinträchtigung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Benachrichtigung vollständig oder teilweise abzusehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Benachrichtigung geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Benachrichtigung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Benachrichtigung etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.
Ähnlich der Beschränkungen in den §§ 11 ff. kann die Benachrichtigung nur „soweit und solange“ aufgeschoben werden, wie die Gefahr für die in Absatz 2 Nummer 1 - 5 genannten Fälle besteht.

Zu Absatz 3

Absatz 3 regelt ein Zustimmungserfordernis ähnlich desjenigen in § 12 Absatz 3, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen (nach Absatz 1 Satz 1 Nummer 4) bezieht. Insofern besteht ein der Situation der aktiven Geltendmachung von Betroffenenrechten vergleichbarer Sachverhalt, weshalb die Übernahme unter Anpassung an die Gegebenheiten des DS-RL geboten ist.

Begründung zu § 49 Auskunftsrecht

§ 49 regelt das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Vorschrift dient mithin der Umsetzung der Artikel 14 und 15 DS-RL. Das Auskunftsrecht setzt – im Gegensatz zu in § 48 angesprochenen aktiven Benachrichtigungspflichten – einen entsprechenden Antrag der betroffenen Person voraus.

Zu Absatz 1

Absatz 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in den Nummern 1 und 4 genannte Begriff „Kategorie“ ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Nummer 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Der Verantwortliche muss sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr zu ermöglichen, aufgrund dieser Informationen zu ermessen, ob die Verarbeitung rechtmäßig ist und – wenn Zweifel hieran bestehen – ggf. die Geltendmachung weitere Betroffenenrechte auf diese Informationen stützen zu können.

Zu Absatz 2

Absatz 2 ist gleichlautend mit § 12 Absatz 2 Satz 2. Die dortigen Ausführungen geltend entsprechend.

Zu Absatz 3

Absatz 3 ist gleichlautend mit § 12 Absatz 1 und dient dem Erhalt der behördlichen Funktionsfähigkeit im Sinne eines Ausuferungsschutzes.

Zu Absatz 4

Absatz 4 normiert, zu welchen Zwecken das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf. Es wird auf die Ausführungen in der Begründung zu § 45 Absatz 2 verwiesen.

Zu Absatz 5

Absatz 5 normiert ein Zustimmungserfordernis wie in § 48 Absatz 3.

Zu Absatz 6

Die Sätze 1 und 2 dienen der Umsetzung von Artikel 15 Absatz 3 Sätze 1 und 2 DS-RL. Satz 3 nimmt in Bezug auf das Absehen von einer Begründung der Auskunftsverweigerung zusätzlich einen aus § 18 Absatz 4 DSG NRW a.F. entnommenen Gedanken auf.

Zu Absatz 7

Absatz 7 regelt die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über die oder den Landesbeauftragten für Datenschutz und Informationsfreiheit ausüben. Dies dient der Umsetzung von Artikel 17 Absatz 1 DS-RL.
Satz 2 sieht in Umsetzung von Artikel 17 Absatz 2 DS-RL eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Absatz 6 berechtigt ist, von einer Information des Antragstellers ganz abzusehen.
Sätze 4 und 5 betreffen den Inhalt der Mitteilungen, die der betroffenen Person seitens der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit zur Verfügung gestellten werden als Ergebnis der dort durchgeführten Prüfung; hier wird Artikel 17 Absatz 3 Satz 1 DS-RL umgesetzt und zur Stärkung der Betroffenenrechte in Satz 5 über das von der Richtlinie Geforderte hinausgegangen, indem die Mitteilung die Information enthalten darf, ob datenschutzrechtliche Verstöße festgestellt wurden, mithin die Auskunftsverweigerung oder teilweise Einschränkung der Auskunft rechtmäßig war. Satz 8 setzt Artikel 17 Absatz 3 Satz 2 DS-RL um.

Zu Absatz 8

Absatz 8 setzt Artikel 15 Absatz 4 DS-RL um.

Begründung zu § 50 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

In § 50 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. Damit wird Artikel 16 DS-RL umgesetzt.

Zu Absatz 1

Absatz 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Dadurch wird Artikel 16 Absatz 1 DS-RL umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 DS-RL enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen; Gleiches gilt etwa für polizeifachliche Bewertungen. In Satz 3 wird Artikel 16 Absatz 3 Satz 1 Buchstabe a DS-RL umgesetzt. Zwar sieht der Richtlinientext im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie beschriebene Sachverhalt systematisch korrekt in

Absatz 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus; vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen substantiiert werden. Dies dient dem Schutz der polizeifachlichen Arbeit und der Vermeidung unverhältnismäßigen Prüfaufwands.

Zu Absatz 2

Absatz 2 normiert das Recht des Betroffenen auf Löschung und dient der Umsetzung von Artikel 16 Absatz 2 DS-RL, in dem sowohl die unabhängig von der Geltendmachung des Betroffenenrechts durch die betroffene Person bestehende Löschungspflicht des Verantwortlichen (s. § 54) als auch das entsprechende Betroffenenrecht angesprochen sind.

Zu Absatz 3

Absatz 3 normiert die Voraussetzungen, unter denen an die Stelle einer Löschung nach Absatz 2 eine Verarbeitungseinschränkung treten kann. Absatz 3 Satz 1 Nummer 3 schafft die Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, wobei diese Regelung als restriktiv auszulegende Ausnahmeregelung anzusehen ist. Im Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT Infrastruktur darauf ausgelegt sein, eine Löschungsverpflichtung auch technisch nachvollziehen zu können.

Satz 2 nimmt einen in § 32 Absatz 5 Satz 2 PolG NRW a.F. enthaltenen Gedanken zur Möglichkeit der Verarbeitung in ihrer Verarbeitung eingeschränkter Daten auf.

Zu Absatz 4

Absatz 4 regelt, dass die Verarbeitungseinschränkung bei automatisierten Dateisystemen sicherzustellen ist und erkennbar sein muss.

Zu Absatz 5

Absatz 5 normiert die Verpflichtung zur Meldung einer Berichtigung der Daten an Stellen, von denen die unrichtigen Daten stammen. Damit wird Artikel 16 Absatz 5 DS-RL umgesetzt. Eine spiegelbildliche Verpflichtung ist in § 54 Absatz 1 für Fälle enthalten, in denen der Verantwortliche von sich aus eine Berichtigung durchzuführen hat unabhängig von der Geltendmachung eines Betroffenen.

Zu den Absätzen 6 und 7

Absatz 6 setzt Artikel 16 Absatz 4 DS-RL um und normiert die Informationspflicht des Verantwortlichen, wenn er einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt. Die Vorschrift ist angelehnt an das Auskunftsrecht in § 49 Absatz 6; demnach wird – so auch in Absatz 7 – weitgehend auf die übereinstimmenden Vorschriften in § 49 zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts verwiesen.

Begründung zu § 51 Verfahren

Die Vorschrift dient der Umsetzung von Artikel 12 DS-RL.

Absatz 1 setzt Artikel 12 Absatz 1, Absatz 2 setzt Artikel 12 Absatz 3, Absatz 3 setzt Artikel 12 Absatz 4 und Absatz 4 setzt Artikel 12 Absatz 5 DS-RL um.

Kapitel 4 Pflichten der Verantwortlichen und Auftragsverarbeiter

Begründung zu § 52 Verarbeitung personenbezogener Daten im Auftrag

Die Norm setzt die Regelungen zur Auftragsdatenverarbeitung nach Artikel 22 DS-RL um. Durch die Verweisung auf Artikel 28 DSGVO werden die dortigen Regelungen zur Auftragsdatenverarbeitung auch bei Verarbeitungen im Anwendungsbereich der DS-RL entsprechend angewendet. Soll eine Datenverarbeitung im Auftrag erfolgen, so ist der Verantwortliche insbesondere dazu verpflichtet, den Auftragsverarbeiter sorgfältig auszuwählen (Artikel 28 Absatz 1 DSGVO). Auch wird in Absatz 1 Satz 2 klargestellt, dass der Auftraggeber für die auf den Auftragnehmer ausgelagerte Verarbeitung verantwortlich bleibt. Die Kernaspekte der Datenverarbeitung, insbesondere ihr Zweck und ihre Dauer, müssen zuvor schriftlich in einem Vertrag oder einem anderen Rechtsinstrument festgelegt werden (Artikel 28 Absatz 3 DSGVO).

Die Absätze 5 bis 8 des Artikel 28 DSGVO wurden von der Verweisung ausgenommen, da die dort zu findenden Bezugnahmen auf Verhaltensregeln und Zertifizierung sowie auf Standardvertragsklauseln im Anwendungsbereich der DS-RL ins Leere gehen.

Zu Absatz 2

Absatz 2 Satz 1 überträgt die obigen Anforderungen an die Auftragsverarbeitung auch auf Fälle, in denen die Prüfung oder Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen durch andere Personen oder Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Dieser Fall wird in der Richtlinie nicht geregelt. Absatz 2 Satz 1 schließt diese Regelungslücke und beugt andernfalls zu erwartenden Rechtsunsicherheiten im Vollzug vor. Zuvor wurde dies durch § 11 Absatz 4 DSG NRW a.F. geregelt, diese Regelung wurde weitestgehend im Absatz 2 Satz 2 ff. übernommen, um ein Absinken des Datenschutzniveaus zu verhindern.

Begründung zu § 53 Verzeichnis von Verarbeitungstätigkeiten

Durch § 53 wird Artikel 24 DS-RL in nationales Recht umgesetzt und eine neue Verpflichtung für Verantwortliche und Auftragsverarbeiter sowie deren Vertreter zur Führung von Verzeichnissen über ihre Verarbeitungstätigkeiten statuiert. Die Vorgaben des Artikel 24 DS-RL sind sowohl was Inhalt als auch Form der Verfahrensverzeichnisse angeht, überwiegend identisch mit den Anforderungen an die Verfahrensverzeichnisse nach Artikel 30 Absatz 1 bis 4 DSGVO und erfahren durch die entsprechende Verweisung Geltung für Verarbeitungen auch im Anwendungsbereich der Richtlinie. Darüber hinaus setzt Artikel 24 Absatz 1 DS-RL ergänzend voraus, dass in dem vom Verantwortlichen zu führende Verarbeitungsverzeichnis die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind, sowie gegebenenfalls die Verwendung von Profiling anzugeben sind. Diese zusätzlichen Anforderungen nach Artikel 24 Absatz 1 DS-RL werden ebenfalls in § 50 umgesetzt.

Begründung zu § 54 Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

§ 54 setzt Artikel 16 DS-RL in seiner Ausformung als Pflicht des Verantwortlichen um. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in § 50.

Zu Absatz 1

In Absatz 1 wird die Pflicht des Verantwortlichen zur Berichtigung aus Artikel 16 Absatz 1 DS-RL umgesetzt.

Zu Absatz 2

Mit diesem Absatz wird Artikel 16 Absatz 2 DS-RL umgesetzt, in dem gleichzeitig das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung angeführt wird. Weiterführend wird auf die Ausführungen zu § 50 Absatz 3 verwiesen.

Zu den Absätzen 3 und 4

Absatz 3 dient der Umsetzung von Artikel 16 Absatz 6 und Artikel 7 Absatz 3 DS-RL. Absatz 4 dient der Umsetzung von Artikel 5 DS-RL.

Begründung zu § 55 Protokollierung

Die Norm dient der Umsetzung von Artikel 25 DS-RL und regelt in Absatz 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Zu den Absätzen 2 und 3

Absatz 2 enthält konkrete Vorgaben an den Inhalt der Protokolle.

Absatz 3 befasst sich mit den Verwendungsbeschränkungen, wobei von der durch die DS-RL eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten anzuwenden, Gebrauch gemacht wird.

Zu Absatz 4

Protokolldateien sind grundsätzlich baldmöglichst zu löschen, wenn diese nicht länger erforderlich sind. Allerdings sind die Protokolldateien gleichfalls ausreichend lange aufzubewahren, um es den Betroffenen zu ermöglichen, die Verarbeitung ihrer Daten zur Überprüfung ihrer Rechtmäßigkeit der Verarbeitung nachvollziehen zu können. Dieser Verpflichtung kommt Absatz 4 mit ausreichender Bemessung zum Ende eines Folgejahres nach Generierung nach.

Zu Absatz 5

Absatz 5 legt fest, dass die Protokolle der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit zum Zweck der Datenschutzkontrolle zur Verfügung gestellt werden müssen.

Begründung zu § 56 Datenschutz-Folgenabschätzung

Die Norm dient der Umsetzung von Artikel 27 DS-RL. In weiten Punkten wurde eine Angleichung der Regelungen zur Umsetzung der DS-RL an die Regelungen der DSGVO angestrebt.

Absatz 1 setzt Artikel 27 Absatz 1 DS-RL um.

Absatz 2 nimmt Artikel 35 Absatz 1 Satz 2 DSGVO auf, Absatz 3 setzt Artikel 35 Absatz 2 der DSGVO um.

Absatz 4 legt den Inhalt der Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 enthaltenen allgemeinen Angaben unter Übernahme der Angaben der in Artikel 35 Absatz 7 DSGVO enthaltenen Punkte.

Absatz 5 nimmt Artikel 35 Absatz 11 DSGVO auf.

Begründung zu § 57 Konsultation des Landesbeauftragten für Datenschutz und Informationsfreiheit

Die Vorschrift dient der Umsetzung von Artikel 28 DS-RL.

Zu Absatz 1

Die Anhörung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit bezweckt die datenschutzrechtliche Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (§ 56), da nach Absatz 1 Nummer 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und der Verantwortliche hierauf nicht mit Maßnahmen zur Gefährdungsminimierung reagiert.

Zu Absatz 2

Der Umfang der Unterlagen, die der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorzulegen sind, wird in Absatz 2 durch Umsetzung der Vorgaben aus Artikel 28 Absatz 4 DS-RL und Artikel 36 Absatz 3 DSGVO konkretisiert.

Zu den Absätzen 3 und 4

Die in Absatz 4 vorgesehene Eilfallregelung trägt solchen operativen und (polizei-) fachlichen Erfordernissen in Abweichung von Absatz 3 Satz 1 Rechnung. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Weiterhin schmälert die Eilfallregelung nicht die der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit zur Verfügung stehenden Befugnisse.

Zu Absatz 5

Absatz 5 dient der Umsetzung von Artikel 28 Absatz 2 DS-RL.

Begründung zu § 58 Anforderung an die Sicherheit der Verarbeitung

§ 58 dient der Umsetzung von Artikel 29 DS-RL.

Zu Absatz 1

Absatz 1 verpflichtet den Verantwortlichen sowie den Auftragsverarbeiter dazu, geeignete technische und organisatorische Maßnahmen für die Sicherheit der Datenverarbeitung zu treffen, insbesondere im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten.
Auch nach § 10 DSG NRW a.F. waren Verantwortlicher und Auftragsverarbeiter verpflichtet, die erforderlichen Maßnahmen zu treffen, um die Ausführungen der Vorschriften dieses Gesetzes zu gewährleisten. Durch die Umsetzung der DS-RL werden die Regelungen konkretisiert, so dass nun Beispiele für solche geeigneten technischen und organisatorischen Maßnahmen benannt werden wie die Pseudonymisierung und Verschlüsselung personenbezogener Daten oder die Instrumente zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit.

Zu Absatz 2

In Absatz 2 werden Inhalte aus Artikel 32 Absatz 1 Buchstabe a bis c DSGVO übernommen. Absatz 2 Satz 1 stellt klar, dass Maßnahmen nur dann erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht und relativiert damit im Kontext der DS-RL die Anwendbarkeit der strengeren Vorschriften der DSGVO.

Zu Absatz 3

Absatz 3 behält das Schutzniveau des DSG NRW a.F. bei. Der Maßnahmenkatalog des § 10 Absatz 2 DSG NRW a.F. wurde hierzu weitestgehend übernommen.

Zu Absatz 4

Der Verantwortliche bzw. der Auftragsdatenverarbeiter werden verpflichtet, bei automatisierten Datenverarbeitungen bestimmte Schutzmaßnahmen zu ergreifen und setzt hierdurch die Vorgaben nach Artikel 29 Absatz 2 DS-RL um. Absatz 3 greift die bereits in der DS-RL vorgesehenen Schutzmaßnahmen auf und ergänzt diese.

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

§ 59 dient der Umsetzung von Artikel 30 DS-RL. Die Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde sind in der Grundverordnung und der Richtlinie weitgehend identisch, so dass durch Verweis auf die weitgehend gleichlautenden Regelungen in Artikel 33 der DSGVO die Regelungen nach Artikel 30 DS-RL umgesetzt werden kann. Satz 2 dient der Umsetzung von Artikel 30 Absatz 6 DS-RL. Eine entsprechende Mitteilungspflicht an den Verantwortlichen eines anderen Mitgliedstaates ist in der Grundverordnung nicht vorgesehen, so dass es hierzu einer gesonderten Umsetzung bedurfte.

Kapitel 5 Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

Begründung zu § 60 Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit

§ 60 setzt Kapitel VI DS-RL um und verweist dazu, wo es möglich ist, auf die Vorschriften der DSGVO und den entsprechenden Vorschriften dieses Gesetzes.

Zu Absatz 1

Absatz 1 dient der Umsetzung von Artikel 41 DS-RL.

Zu Absatz 2

Absatz 2 Satz 1 setzt Artikel 46 DS-RL um. Satz 2 dient der Umsetzung von Artikel 46 Absatz 1 Buchstabe g) DS-RL, welcher durch den Verweis in die DSGVO in Satz 1 nicht mit abgedeckt wird.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 47 DS-RL.

Zu Absatz 4

Absatz 4 trägt dem Umstand Rechnung, dass der Jahresbericht nach Artikel 49 Satz 1 der Richtlinie auch eine Liste der Arten der verhängten Sanktionen enthalten kann.

Begründung zu § 61 Recht auf Beschwerde bei einer Aufsichtsbehörde

§ 61 dient der Umsetzung von Artikel 52 DS-RL.

Satz 1 setzt die Vorgaben des Artikel 52 Absätze 1 und 4 durch entsprechende Verweisung auf die nahezu wortgleiche Vorschrift des Artikel 77 DSGVO um. Die Sätze 2 und 3 setzen darüber hinaus die weitergehenden Vorgaben nach Artikel 52 Absätze 2 und 3 DS-RL in nationales Recht um. Sie betreffen den Fall einer Beschwerde, für die eine andere Aufsichtsbehörde zuständig ist. Die weitere Unterstützung durch die Aufsichtsbehörde im Sinne des Satzes 3 umfasst gemäß Erwägungsgrund 81 DS-RL lediglich die Information der betroffenen Person über den Zwischenstand ggf. erfolgter weiterer Untersuchungen.

Kapitel 6 Datenübermittlungen an Drittstaaten und an internationale Organisationen

Begründung zu § 62 Allgemeine Voraussetzungen

§ 62 dient der Umsetzung von Artikel 35 DS-RL und statuiert Voraussetzungen, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Darüber hinaus enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen - auch an die insbesondere nach den §§ 63 bis 65 erforderliche Abwägungsentscheidung - aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u. 1 BvR 1140/06). In besonderer Ausprägung dessen fordert Absatz 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht, dass ein elementaren

rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist; hierbei ist - unter Übernahme eines Gedanken aus § 14 Absatz 7 BKAG a. F. - besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

Begründung zu § 63 Datenübermittlung bei geeigneten Garantien

§ 63 dient der Umsetzung von Artikel 37 DS-RL. In § 63 werden § 62 ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt dem Verantwortlichen – insbesondere nach § 63 Absatz 1 Absatz 1 Nummer 2 – die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Die etwa beim Bundeskriminalamt bestehende Praxis, nach einer solchen Beurteilung die Datenübermittlung mit der Mitgabe von Verarbeitungsbedingungen – etwa Löschverpflichtungen nach Zweckerreichung, Weiterübermittlungsverbote, Zweckbindungen – zu verbinden, ist dazu geeignet, diese Beurteilung zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren § 62 Absatz 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Zu Absatz 2

Absatz 2 dient der Umsetzung von Artikel 37 Absatz 3 DS-RL zur Dokumentation der Übermittlungen nach § 63.

Zu Absatz 3

Absatz 3 dient der Umsetzung von Artikel 37 Absatz 2 DS-RL, der die Unterrichtung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit über Kategorien von Übermittlungen vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

Begründung zu § 64 Datenübermittlung ohne geeignete Garantien

§ 64 dient der Umsetzung von Artikel 38 DS-RL und beleuchtet Konstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 63 erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Begründung zu § 65 Sonstige Datenübermittlung an Empfänger in Drittstaaten

§ 65 dient der Umsetzung von Artikel 39 DS-RL. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen „im besonderen Einzelfall“ gelten die in § 63 Absatz 1 genannten strengen Voraussetzungen. In Absatz 4 ist eine verstärkte Zweckbindung der gemäß § 63 übermittelten Daten vorgesehen.

Kapitel 7 Ergänzende Vorschriften

Begründung zu § 66 Vertrauliche Meldung von Datenschutzverstößen

§ 66 setzt Artikel 48 DS-RL in Landesrecht um. Die Vorschrift dient dem Schutz von Informanten, die Kenntnis von Datenschutzpannen und Datenschutzverstößen erlangt haben. Durch die Gewährleistung einer vertraulichen Behandlung sollen Meldungen über diese unterstützt werden.
Der Verantwortliche hat dafür zu sorgen, dass ein entsprechendes Verfahren zur Verfügung gestellt wird, das sowohl verwaltungsinterne Meldungen als auch Hinweise von betroffenen Personen oder sonstigen Dritten vertraulich behandelt werden. Welche Maßnahmen der Verantwortliche im Einzelnen ergreift, steht in seinem Ermessen.

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

Die Bestimmungen der Richtlinie orientieren sich insbesondere in Bezug auf die Ausgestaltung von Verfahrens- und Organisationsregelungen weitgehend an denen der DSGVO.
Im Interesse einer vereinfachten Anwendung und um die Fehleranfälligkeit bei der Abgrenzung zwischen DSGVO und DS-RL zu reduzieren, werden daher im Wege einer Verweisung die entsprechenden Regelungen der Grundverordnung für Verarbeitungen im Anwendungsbereich der Richtlinie zur Anwendung gebracht.

Begründung zu § 68 Schadensersatz

Die Vorschrift dient der Umsetzung des in Artikel 56 DS-RL vorgesehenen Rechts der betroffenen Person auf Schadensersatz bei rechtswidrigen Datenverarbeitungen. Anders als die Datenschutzrichtlinie 95/46/EG sieht Artikel 56 DS-RL keine Exkulpationsmöglichkeit für den Verantwortlichen vor, sondern etabliert eine verschuldensunabhängige Gefährdungshaftung.

Zu Absatz 1

Absatz 1 Satz 1 entspricht § 20 Absatz 1 Satz 1 DSG NRW a.F. Gemäß Satz 2 entfällt die Ersatzpflicht, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist. Da die nicht automatisierte Verarbeitung gemäß Artikel 2 Absatz 2 DS-RL nicht in den Anwendungsbereich der DS-RL fällt, ist für diesen Bereich eine von Artikel 56 DS-RL abweichende Regelung möglich.

Zu Absatz 2

In Abänderung von § 20 Absatz 1 Satz 2 DSG NRW a.F. normiert Absatz 2 einen Anspruch auf Schadensersatz bei erlittenen immateriellen Schäden unabhängig von der Schwere der Fälle. Ein Anspruch auf Schadensersatz war nach bisher geltendem Recht nur in schweren Fällen von Schäden die nicht Vermögensschäden sind möglich. Artikel 56 DS-RL und Erwägungsgrund 88 schaffen die Unterscheidung zwischen materiellen und immateriellen Schäden nunmehr ab.

Zu den Absätzen 3 bis 5

Die Absätze 3 bis 5 orientieren sich an § 20 Absätze 2 bis 3 DSG NRW a.F. und führen in Teilen die geltende Rechtslage fort. Absatz 5 lässt dabei die Haftung nach anderen Vorschriften, unberührt.

Begründung zu § 69 Straf- und Bußgeldvorschriften

§ 69 dient der Umsetzung von Artikel 57 DS-RL, wonach die Mitgliedstaaten Verstößen gegen die aufgrund der Richtlinie erlassenen nationalen Vorschriften mit Sanktionen ahnden können. Die Vorschriften gegen Verstöße der DSGVO in §§ 33, 34 dieses Gesetzes finden entsprechend im Anwendungsbereich des § 35 und damit im Anwendungsbereich der DS-RL Anwendung, so dass in dieser Hinsicht ein Gleichklang zwischen DSGVO und DS-RL erzielt werden kann.

Teil 4 Übergangsvorschrift, Einschränkung von Grundrechten, Inkrafttreten, Außerkrafttreten

Begründung zu § 70 Übergangsvorschrift

Zu Absatz 1

Mit Absatz 1 wird eine Übergangsregelung für die zum Zeitpunkt des Inkrafttretens des Gesetzes im Amt befindliche Landesbeauftragte geschaffen. Hierdurch wird zum einen die Wahlperiode der derzeitigen Landesbeauftragten für Datenschutz und Informationsfreiheit und damit die damalige Entscheidung des Landtages unangetastet gelassen; andererseits wird ihre Stellung mit Geltung der vorrangigen DSGVO entsprechend angepasst.

Zu den Absätzen 2 und 3

Auf der Basis des Artikels 63 Absatz 2 DS-RL mit Erwägungsgrund 96 DS-RL berücksichtigen die Absätze 2 und 3, die sich aus der Datenschutzreform ergebenden weitreichenden Änderungen für IT-Verfahren im Land. Die Absätze 2 und 3 betreffen nur Fachverfahren öffentlicher Stellen im Anwendungsbereich des Teiles 3 dieses Gesetzes.
Insbesondere die in den §§ 42 bis 45 neu ausgeformten Personenkategorien, Datenquellenangaben und besonderen Datenschutzkategorien sowie die neuen Dokumentationspflichten (§ 53), Prüfroutinen (§ 54) und Protokollierungen (§ 55) zu IT-Verfahren werden alleine in der praktischen Umsetzung bezüglich der über 120 zentralen und über 500 dezentralen IT-Verfahren der Polizei NRW zu erheblichen Anpassungs-Aufwänden führen, die beim Zwang zu einer raschen Umsetzung zu Lasten anderer operativer Aufgabenerfüllungen gehen werden.
Zur Abfederung dieser erheblichen Auswirkungen und zur Etablierung einer gesicherten Auslegung der neuen Vorschriften nimmt NRW die Umsetzungsfrist nach Artikel 63 Absatz 2 DS-RL, bis zum 6. Mai 2023, in Anspruch und schafft auf diese Weise für Verantwortliche und Auftragsdatenverarbeiter (Erwägungsgrund 96 DS-RL) eine angemessene Übergangsregelung für den Umgang mit Bestandsverfahren. Bis zum 6. Mai 2023 gelten demnach die Regelungen, nach denen die Bestandsverfahren eingeführt worden sind. Bis zum Ablauf der Frist sind sämtliche IT-Verfahren in NRW im Anwendungsbereich des Teiles 3 dieses Gesetzes allerdings mit den Voraussetzungen der §§ 53 und 55 in Einklang zu bringen.

Begründung zu § 71 Einschränkung von Grundrechten

Die Regelung in § 71 dient der Umsetzung des Zitiergebots aus Artikel 4 Absatz 1 Landesverfassung Nordrhein-Westfalen i.V.m. Artikel 19 Absatz 1 Grundgesetz.

Begründung zu § 72 Inkrafttreten, Außerkrafttreten

Da die DSGVO nach Artikel 99 Absatz 2 DSGVO ab dem 25. Mai 2018 unmittelbar geltendes Recht in Deutschland ist, treten mit Absatz 1 das neue, sie ergänzende DSG NRW zu diesem Zeitpunkt in Kraft. Gleichzeitig tritt das geltende DSG NRW außer Kraft.

Begründung zu Artikel 2 Änderung des Gesetzes über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen

Zu Nummer 1 (§ 10 Einwilligung der betroffenen Person)

§ 10 wird an die Änderungen des Datenschutzrechts durch die europäische Datenschutzreform angepasst. Die für Nordrhein-Westfalen geltenden Regelungen des Datenschutzes finden sich nun nicht mehr nur im DSG NRW, sondern u.a. auch in der unmittelbar und vorrangig geltenden DSGVO, so dass der Verweis allein auf § 4 DSG NRW a.F. nicht mehr zutreffend ist. Durch den Verweis in das jeweils geltende Datenschutzrecht bleibt im Grundsatz die bisherige Vorgabe, geeignete Maßnahmen zur Abtrennung von Informationen ergreifen zu sollen, erhalten.

Zu Nummer 2 (§ 13 Beauftragte oder Beauftragter für das Recht auf Information)

Da das Datenschutzgesetz NRW (DSG NRW) wegen der europäischen Datenschutzreform (DSGVO und DS-RL) grundlegend überarbeitet wird und sich an den veränderten Vorgaben des europäischen Datenschutzrechts zu orientieren hat, wird die bisher bestehende Regelung in § 13 Absatz 2 Satz 2 IFG NRW, die eine entsprechende Geltung des DSG NRW für das IFG NRW vorsieht, in dieser Form nicht mehr möglich sein.

Um den für die Anwendung des IFG NRW notwendigen Regelungsgehalt aus dem (bisherigen) DSG NRW auch künftig anwendbar zu machen, werden das Anrufungsrecht und die einschlägigen Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit im Wege einer Vollregelung nunmehr in § 13 normiert. Im Bereich des IFG NRW bleibt die Beanstandung die Maßnahme, um in schärfster Form auf Rechtsverstöße im Bereich des IFG NRW zu reagieren. Einen modifizierten Verweis auf das DSG NRW enthält im Übrigen § 13 Absatz 3 bezogen auf die „Berufung“ und „Rechtsstellung“ der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit. Insoweit ist ein Verweis entsprechend der bisherigen Rechtstradition möglich und sinnvoll, damit Doppeltregelungen vermieden werden.

Begründung zu Artikel 3 Änderung des Meldegesetzes für das Land Nordrhein-Westfalen

Zu Nummer 1 (Inhaltsübersicht)

Die Änderung der Inhaltsübersicht ist aufgrund der Änderungen unter Nummer 2 erforderlich.

Zu Nummer 2 (§ 2 Verarbeiten von Daten)

Bei diesen Anpassungen handelt es sich um redaktionelle Anpassungen an die ab dem 25. Mai 2018 unmittelbar geltende DGSVO und der darin verwendeten Terminologie.

Zu Nummer 3 (§ 7 Verfahren des automatisierten Abrufs durch Behörden)

Die Regelung erfolgt zur Anpassung an die europäische Datenschutzreform. Der automatisierte Abruf von Daten ist gemäß § 6 Absatz 1 DSG NRW nur zulässig, soweit die Verarbeitung zur Erfüllung eines Zwecks des Artikels 6 Absatz 1 Buchstabe c oder e DSGVO erfolgt. Im vorliegenden Fall erfolgt das Bereithalten der Daten zum automatisierten Abruf nach Artikel 6 Absatz 1 Buchstaben c) und e) DSGVO, da das Bereithalten von Daten zum automatisierten Abruf durch die Meldebehörden über das Meldeportal Behörden sowohl der Erfüllung der rechtlichen Verpflichtung nach § 39 Absatz 3 Bundesmeldegesetz als auch der Erfüllung der öffentlichen Aufgaben der abrufenden Stellen dient.

Begründung zu Artikel 4 Änderung des Ausführungsgesetzes NRW Glücksspielstaatsvertrag

Bei dieser Regelung handelt es sich um eine redaktionelle Anpassung an die ab dem 25. Mai 2018 unmittelbar geltende DSGVO.
Die Verantwortlichkeit der Veranstalter von Glücksspielen, die eine Sperre aussprechen und damit ebenfalls Daten der Spielerinnen und Spieler verarbeiten, folgt unmittelbar aus Artikel 4 Nummer 7 DSGVO.

Begründung zu Artikel 5 Änderung des Spielbankgesetzes NRW

Bei dieser Regelung handelt es sich um eine redaktionelle Anpassung an die ab dem 25. Mai 2018 unmittelbar geltende DSGVO.
Die Verantwortlichkeit der Veranstalter von Glücksspielen, die eine Sperre aussprechen und damit ebenfalls Daten der Spielerinnen und Spieler verarbeiten, folgt unmittelbar aus Artikel 4 Nummer 7 DSGVO.

Begründung zu Artikel 6 Änderung des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen

Zu Nummer 1 (Inhaltsübersicht)

Die Änderung der Inhaltsübersicht ist aufgrund der Aufhebung des Satzes 2 in § 3b erforderlich.

Zu Nummer 2 (§ 3b Personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse)

§ 3b Satz 2 VwVfG NRW regelt, dass die Behörde, soweit sie personenbezogene Daten verarbeitet, den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) unterliegt.

Diese Regelung wurde ursprünglich in § 3a Satz 2 VwVfG NW kodifiziert. Sie wurde durch Artikel 3 des Gesetzes zur Fortentwicklung des Datenschutzes (GFD) vom 15.03.1988 (GV. NW. S. 160), das als Kernstück in Artikel 1 das Datenschutzgesetz NW (DSG NW) enthielt, in das damalige VwVfG NW aufgenommen. Die bis dahin in § 30 VwVfG NW enthaltene und aufgrund ihrer systematischen Stellung in Teil 2 des VwVfG NW auf Verwaltungsverfahren im Sinne des § 9 VwVfG NW beschränkte Regelung zur Geheimhaltung von Angaben über persönliche und sachliche Verhältnisse und zur Wahrung von Betriebs- und Geschäftsgeheimnissen wurde als neuer § 3a Satz 1 VwVfG NW in Teil 1 des VwVfG NRW übertragen. Gleichzeitig wurde die Regelung inhaltlich um den hier in Rede stehenden Satz 2 erweitert. Dadurch wurde die Verbindung zu den für die datenschutzrechtliche Beurteilung von Datenübermittlungen bislang maßgeblichen Vorschriften des Datenschutzgesetzes hergestellt. Es sollte deutlicher herausgestellt werden, dass die Beachtung des Datenschutzes für jedwede Behördentätigkeit und damit über die in § 9 VwVfG NRW normierten Verwaltungsverfahren (Erlass eines Verwaltungsakts bzw. Abschluss eines öffentlich-rechtlichen Vertrags) hinaus gilt.

Durch Artikel 1 des Elektronik-Anpassungsgesetzes vom 06.07.2004 (GV. NRW. S. 370) wurde § 3a VwVfG NRW bei identischem Inhalt redaktionell zu § 3b VwVfG NRW umbenannt.

Mit Anwendbarkeit der DSGVO wird diese ab dem 25. Mai 2018 im nationalen Recht unmittelbar gelten und Vorrang gegenüber dem nationalen Recht genießen. Das DSG NRW wird die DSGVO künftig nur noch ergänzen. Ein ausdrücklicher Hinweis im VwVfG NRW darauf, dass das Behörden, soweit sie personenbezogene Daten verarbeiten, dem DSG NRW unterliegen, könnte zu Fehlinterpretationen dahingehend führen, dass der Datenschutz sich nach wie vor

ausschließlich nach dem DSG NRW richte. Darüber hinaus bedarf es im Gegensatz zu der Situation im Jahr 1988, in der das Datenschutzgesetz NW (erstmals) verkündet wurde, eines klarstellenden Hinweises im VwVfG NRW auf die Verpflichtung zur Wahrung des Datenschutzes mittlerweile nicht mehr.

Die Aufhebung der Regelung liegt außerdem im Interesse der in den Verwaltungsverfahrensgesetzen von Bund und Ländern praktizierten Konkordanzgesetzgebung. Die Übereinstimmung der Verwaltungsverfahrensgesetze von Bund und Ländern im Wortlaut ist Voraussetzung für die Rückführung und Vermeidung verfahrensrechtlicher Sonderregelungen im materiellen Bundesrecht. Nach § 137 Absatz 1 Nummer 2 der Verwaltungsgerichtsordnung (VwGO) ist die Übereinstimmung im Wortlaut zudem Voraussetzung für die Revisibilität der Landesverwaltungsverfahrensgesetze und dient damit der einheitlichen Auslegung der Vorschriften durch die Gerichte. Auch im Verwaltungsverfahrensgesetz des Bundes findet sich kein Hinweis auf eine behördliche Verpflichtung zur Beachtung des Datenschutzes; diese wird vielmehr als selbstverständlich vorausgesetzt.

Zu Nummer 3 (§ 26 Beweismittel)

Auch die Ergänzung in § 26 Absatz 2 Satz 3 VwVfG NRW, wonach im Rahmen der Mitwirkungspflicht der Beteiligten bei der Ermittlung des Sachverhalts im Verwaltungsverfahren eine Pflicht zur Angabe von personenbezogenen Daten nur besteht, soweit sie durch Rechtsvorschrift besonders vorgesehen ist, wurde durch Artikel 3 des Gesetzes zur Fortentwicklung des Datenschutzes (GFD) vom 15.03.1988 (GV. NW. S. 160) eingeführt. Nach der Gesetzesbegründung (Drs. 10/1565) sollte klargestellt werden, dass die betroffene Person zu einer Offenbarung personenbezogener Daten entsprechend der Rechtsprechung des Bundesverfassungsgerichts (Grundsatzentscheidung vom 15.12.1983 zum Volkszählungsgesetz - BVerfGE 65,1) nur verpflichtet ist, soweit dies gesetzlich geregelt ist. Einer solchen Klarstellung bedarf es heute nicht mehr.

Auch in § 26 Absatz 2 Satz 3 des VwVfG des Bundes ist diese datenschutzrechtliche Regelung nicht enthalten. Eine entsprechende Anpassung des § 26 Absatz 2 Satz 3 VwVfG NRW liegt somit auch hier im Interesse der Konkordanzgesetzgebung.

Begründung zu Artikel 7 Änderung des Landesbeamtengesetzes

Zu Nummer 1 (Inhaltsübersicht)

In der Inhaltsübersicht werden die Angaben zu den §§ 86 und 87 sprachlich angepasst.

Zu Nummer 2 (§ 83 Personalakten - allgemein)

Zu Absatz 1

Satz 2: Es handelt sich um eine begriffliche Anpassung an Artikel 4 Nummer 2 DSGVO.
Satz 7: Es handelt sich um eine begriffliche Anpassung an Artikel 4 Nummer 2 DSGVO.

Zu Absatz 4

Satz 1: Es handelt sich nun bei der Vorschrift um eine zentrale Ermächtigungsnorm. Die bereichsspezifische Datenschutzregelung erlaubt es dem Dienstherrn, personenbezogene Daten über die Beamtin oder den Beamten zu verarbeiten. Der Regelungsinhalt wird erweitert.

„Verarbeiten“ bedeutet demnach: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“

Als Zweck der Verarbeitung werden nun die Begrifflichkeiten Personalverwaltung und Personalwirtschaft verwendet. Die DSGVO legt den Fokus stark auf die Datenverarbeitung ausschließlich zu den gesetzlichen definierten Zwecken. Um hier Probleme bei der Auslegung zu minimieren, wird der Zweck entsprechend der DSGVO definiert.

Personalakten dürfen grundsätzlich ohne Einwilligung der Beamtin oder des Beamten nur für Zwecke der Personalverwaltung und der Personalwirtschaft verwendet werden.

Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt. Eine die Mitbestimmung des § 72 Absatz 3 LPVG ausschließende erschöpfende gesetzliche Regelung enthält § 83 Absatz 4 LBG-E daher nach wie vor nicht.

Zu Nummer 3 (§ 84 Beihilfeakten)

Es handelt sich um eine begriffliche Anpassung an Artikel 4Nummer 2 EU DS-GVO.

Zu Nummer 4 (§ 86 Auskunftsrecht)

Die Überschrift und die weiteren Absätze werden hinsichtlich der Begrifflichkeit „Auskunftsrecht“ aus der DSGVO angepasst.

Zu Absatz 1

Der Anspruch auf Auskunft ergibt sich unmittelbar aus der DSGVO, daher darf dieser wegen des Wiederholungsverbots im nationalen Recht nicht mehr geregelt werden. Das Recht auf Einsicht in die Personalakte ist ein besonderes Auskunftsrecht im Sinne der DSGVO. Das Recht auf Einsicht in die Personalakte als spezifisch beamtenrechtliche Konkretisierung des Anspruchs auf Auskunft bzw. des verwaltungsverfahrensrechtlichen Rechts auf Anhörung und Akteneinsicht beruht auf den Prinzipien der Menschenwürde und des rechtlichen Gehörs und kann vom Schutzzweck her auch vom Schutzzweck der DSGVO abgegrenzt werden. Absatz 4 ist nun in Absatz 1 aufgenommen worden. Der Begriff Einsichtnahme wird durch Auskunft ersetzt.

Zu Absatz 2

Es handelt sich um Anpassung an den Regelungsinhalt des Absatzes 1.

Zu Absatz 3

Das Schutzniveau des Betroffenenrechts wird im Sinne der DSGVO durch das Einfügen des Wortes „wichtige“ erhöht und betont.

Zu Nummer 5 (§ 87 Übermittlung und Auskunft an nicht betroffene Personen)

Die Überschrift und der Text der Regelung werden an die Begrifflichkeiten aus Artikel 4 und 15 der DSGVO angepasst.

Zu Nummer 6 (§ 89 Verarbeitung und Übermittlung von Personalaktendaten)

Die DSGVO verwendet den Begriff des automatisierten Verfahrens, die Vorschrift wird daher an die Begrifflichkeiten angepasst.

Zu Absatz 2

Durch die Neufassung wird klargestellt, dass die sonstigen Vorschriften des Personalaktenrechts (Beihilfeakte § 84) gerade auch dann gelten, wenn der Akteninhalt im automatisierten Verfahren verarbeitet wird. Insbesondere die Weitergabe der Beihilfedaten für andere als für Beihilfezwecke im automatisierten Verfahren soll nur unter den im § 84 genannten Voraussetzungen sowie für den Fall der teilweisen (z.B. Prüfung von Rechnungen bestimmter medizinischer Leistungserbringer wie z.B. Krankenhäuser) oder umfänglichen Übertragung von Aufgaben der Beihilfebearbeitung möglich sein.

Zu Nummer 7 (§ 91 Übertragung von Aufgaben der Personalverwaltung)

Die Vorschrift wird an die Regelungssystematik der europäischen Datenschutzreform angepasst. Das DSG NRW trifft keine eigene Regelung zur Auftragsverarbeitung mehr, da Artikel 28 DSGVO dies nunmehr abschließend regelt.

Zu Nummer 8 (§ 91 a Verarbeitung von Personalakten im Auftrag)

Die Vorschrift wird an die Regelungssystematik der europäischen Datenschutzreform angepasst.

Begründung zu Artikel 8 Änderung des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz

Zu Nummer 1 (§ 30 Externe Notfallpläne für schwere Unfälle mit gefährlichen Stoffen)

In § 30 Absatz 3 Satz 2 erfolgt lediglich eine Begriffsanpassung an die Terminologie der DSGVO und des Datenschutzgesetztes Nordrhein-Westfalen. Das Wort „Angaben“ wird durch das Wort „Daten“ ersetzt.

Zu Nummer 2 (§ 46 Verarbeitung personenbezogener Daten)

Zu Absatz 1

Er beinhaltet die aktualisierte Verweisung auf das geltende Datenschutzrecht.

Zu Absatz 2

Absatz 2 Satz 3 wird eine gesetzliche Ermächtigung für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 DSGVO eingefügt. Hierunter fallen beispielsweise personenbezogene Daten, aus denen die rassische und ethnische Herkunft hervorgeht, oder Gesundheitsdaten. Es kann nicht ausgeschlossen werden, dass solche Daten im Einzelfall anfallen, etwa im Zusammenhang der Entgegennahme eines Notrufs oder mit der Datenerhebung bei den Personenauskunftsstellen.

Das Verarbeitungsverbot nach Artikel 9 Absatz 1 DSGVO gilt auf Grundlage des Artikels 9 Absatz 2 Buchstaben c und g DSGVO vorliegend nicht. Die hierdurch zulässige Verarbeitung

personenbezogener Daten dient insbesondere bei Notrufen dem Schutz lebenswichtiger Interessen des Betroffenen und steht damit in einem angemessenen Verhältnis zur Wahrung seiner Grundrechte.

Zu Absatz 3

Die Regelung des Absatzes 3 Satz 1 beschränkt gemäß Artikel 23 Absatz 1 DSGVO die Informationspflichten des Verantwortlichen zur Sicherstellung einer sachgerechten Aufgabenwahrnehmung und effektiven Gefahrenabwehr sowie zum Schutz von Leib und Leben (vgl. insbesondere Artikel 23 Absatz 1 Buchstabe c und I DGSVO).

Zu Absatz 4

Die Regelung in Absatz 4 ist inhaltlich unverändert. Eine Verweisung auf das Datenschutzgesetz Nordrhein-Westfalen ist an dieser Stelle aufgrund der Regelung in § 46 Absatz 1 entbehrlich.

Zu den Absätzen 5 und 6

Die bisherige Regelung in § 46 Absatz 5 wird aufgehoben, da die DSGVO und das Datenschutzgesetz Nordrhein-Westfalen bereits Regelungen zur unverzüglichen Löschung der Daten enthalten.

Bei den Anpassungen in den bisherigen Absätzen 6 und 7 (Änderung der Nummerierung) handelt es sich um redaktionelle Anpassungen.

Der bisherige Verweis in dem bisherigen § 46 Absatz 7 Satz 2 auf das Datenschutzgesetz Nordrhein-Westfalen ist an dieser Stelle aufgrund der neuen Regelung in § 46 Absatz 1 entbehrlich.

Begründung zu Artikel 9 Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen

A Allgemeiner Teil

Als Ausfluss geänderten EU-Rechts und der diesbezüglichen Novellierung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) sollen die bereichsspezifischen datenschutzrechtlichen Regelungen des Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG NRW) angepasst und zum Teil neu gefasst werden.

Mit Inkrafttreten 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 – DSGVO) am 25. Mai 2018 wird das bisherige DSG NRW in vielen Bereichen durch EU-Recht abgelöst (s. § 69 DSG NRW-neu). Die DSGVO gilt unmittelbar in den Mitgliedstaaten der Europäischen Union für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen. Nicht in dessen Anwendungsbereich fallen Tätigkeiten, welche die nationale Sicherheit betreffen, wie etwa die Datenverarbeitung im Bereich des VSG NRW.

Das bisherige DSG NRW tritt zum 25. Mai 2018 außer Kraft. Das neue DSG NRW trifft ergänzende Regelungen zur DSGVO und dient 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. EU L 119 vom 4. Mai 2016, S. 89).

Durch Aufnahme bereichsspezifischer Regelungen und den Verweis auf das Bundesdatenschutzgesetz (BDSG) in der Fassung vom 30. Juni 2017 (BGBl. I S. 2097) in das nordrhein-westfälische VSG wird eine bereichsspezifische Vollregelung für die Verfassungsschutzbehörde geschaffen, die abschließend ist und eine subsidiäre Geltung der nicht direkt anwendbaren Verordnung (EU) 2016/679 ausschließt. Ein Verweis auf das DSG NRW-neu unterbleibt, da dieses auf den Anwendungsbereich der DSGVO zugeschnitten ist und darauf bezogene Durchführungsbestimmungen und ergänzende Regelungen trifft. Es enthält kein eigenständiges Regelungswerk mehr für Bereiche, die außerhalb des Anwendungsbereichs des Unionsrechts liegen.

Da das BDSG-neu hingegen auch die Rechtsbereiche eigenständig regelt, die außerhalb des Unionsrechts liegen und daher weder der DSGVO noch der Richtlinie (EU) 2016/680 unterfallen (BT-Drs. 18/11325, S. 74), wird im Interesse eines kohärenten und anwenderfreundlichen Datenschutzrechts im Bereich des VSG NRW auf die bundesrechtlichen Regelungen verwiesen. Damit wird einerseits eine „Zersplitterung“ der Rechtsanwendung im Bereich des VSG NRW durch ein Nebeneinander der DSGVO, des landesrechtlichen DSG und des Spezialrechts im VSG NRW vermieden. Andererseits kann darüber hinaus angesichts einer angestrebten Harmonisierung der wesentlichen Regelungen der Verfassungsschutzgesetze des Bundes und der Länder bereits jetzt im Bereich der datenschutzrechtlichen Normen ein Gleichklang mit dem schon angepassten Bundesverfassungsschutzgesetz (BVerfSchG), das ebenfalls auf das BDSG-neu verweist, hergestellt werden.

Neue bereichsspezifische Regelungen im VSG NRW betreffen u.a. die Datenschutzkontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit sowie die Ausgestaltung von Verfahrensverzeichnissen. Im Übrigen wird insbesondere hinsichtlich des Grundsatzes der Einwilligung und des Datengeheimnisses, der automatisierten Einzelentscheidungen und Abrufverfahren, der Auftragsverarbeitung und der Sicherheit der Datenverarbeitung auf das neue Bundesdatenschutzgesetz verwiesen.

B Besonderer Teil

Zu § 5 Absatz 1

§ 5 Absatz 1 wird um einen Satz ergänzt, der die Verarbeitung personenbezogener Daten bei Einwilligung des Betroffenen für zulässig erklärt. Der Grundsatz der Einwilligung wurde bisher von § 4 Absatz 1 Buchstabe b DSG NRW-alt geregelt. Die DSGVO enthält diesen Grundsatz in Artikel 6 Absatz 1 Buchstabe a. Für die Einzelheiten der Einwilligung verweist § 31 Absatz 2 VSG NRW auf § 51 Absatz 1 bis 4 BDSG-neu.

§ 51 Absatz 5 BDSG-neu trifft eine Regelung zur Einwilligung bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Da der Umgang mit diesen dort bezeichneten Daten für die Verfassungsschutzbehörde aufgabentypisch ist, erfolgt ein Verweis auf § 51 Absatz 5 BDSG-neu nicht. § 51 Absatz 4 BDSG-neu enthält das Gebot der Freiwilligkeit der Einwilligung. Entsprechend der Gesetzesbegründung des Bundes zu § 8 Absatz 1 Satz 1 BDSG-neu (BT-Drs. 18/11325, S. 122) besteht auch ein Koppelungsverbot, wonach Vor- oder Nachteile nicht sachwidrig von einer Datenverarbeitungserlaubnis abhängen dürfen.

Zu § 5c

a) Absatz 2

Die Änderung in Absatz 2 ist eine Folgeänderung der neuen Begriffsdefinition in § 46 Nummer 3 BDSG-neu. Die „Einschränkung der Verarbeitung“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die Wörter, „sperren“ (d.h. das Verhindern der weiteren Verarbeitung gespeicherter Daten) und „kennzeichnen“ werden daher durch die Begriffe „die Verarbeitung einschränken“ ersetzt.

b) Absatz 4 Satz 1 und Satz 2

Die Regelung entspricht dem mit Artikel 6 des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097) ergänzten § 4 Absatz 4 Satz 1 Artikel 10-Gesetz (G 10), der am 25. Mai 2018 in Kraft tritt. Dort wird klargestellt, dass sich die restriktive Übermittlungsregelung nur auf „andere als die nach § 1 Absatz 1 Nummer 1 berechtigten Stellen“ beziehe, womit insbesondere die Exekutivbehörden gemeint sind. Die weitere Verwendung der Daten zur nachrichtendienstlichen Aufklärung der gemäß § 1 Absatz 1 Nummer 1 Artikel G 10 drohenden Gefahren ist laut Gesetzesbegründung zur Änderung des G 10 dagegen in § 4 Absatz 2 Satz 3 G 10 auch für den Fall der Übermittlung geregelt.

Die Übernahme der Regelung in § 5c Absatz 4 stellt auch für die nordrhein-westfälische Verfassungsschutzbehörde klar, dass die restriktiven Übermittlungsvorschriften von Erkenntnissen aus G 10-Maßnahmen nur für die Weitergabe an Behörden außerhalb der inländischen Nachrichtendienste unter den dort genannten Voraussetzungen gelten, nicht aber bei der weiteren Verwendung zur nachrichtendienstlichen Aufklärung der in §§ 7a Absatz 1 oder § 7c Absatz 1 genannten drohenden Gefahren.

c) Absatz 4 Satz 3

Es handelt sich um die Umsetzung des mit Artikel 6 des DSAnpUG-EU vom 30. Juni 2017 (BGBl. I S. 2097) um Satz 2 ergänzten § 4 Absatz 4 G 10, der am 25. Mai 2018 in Kraft tritt. Dort wird bei Übermittlung an ausländische Stellen § 19 Absatz 3 Satz BVerfSchG für anwendbar erklärt. Die Regelung des § 19 Absatz 3 Satz BVerfSchG wird in den neuen Satz 2 des Absatzes 4 aufgenommen und zur Klarstellung um einen Verweis auf § 5 Absatz 5 Satz 2 BVerfSchG ergänzt, der den Dienstverkehr der Landesverfassungsschutzbehörden mit öffentlichen Stellen anderer Staaten regelt.

Zu § 10

Die Änderungen in der Überschrift und in Absatz 2 Satz 4 sind Folgeänderungen der neuen Begriffsdefinitionen in § 46 BDSG-neu.

Zu § 11

Die Änderungen in der Überschrift sowie in den Absätzen 2 bis 4 sind Folgeänderungen der neuen Begriffsdefinitionen in § 46 BDSG-neu.

Zu § 12

§ 12 wird einschließlich seiner Überschrift neu gefasst.

a) Absatz 1

Beim Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten ist bisher § 8 DSG NRW in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542), zuletzt geändert durch Artikel 1 des Gesetzes vom 11. Juli 2011 (GV. NRW. S. 338), zu beachten. § 12 greift die Regelung des § 70 BDSG-neu bereichsspezifisch im Verfassungsschutzgesetz NRW auf.

Anders als im bisherigen § 8 Absatz 2 DSG NRW-alt sieht § 12 kein grundsätzliches Einsichtsrecht für jedermann vor. Die Rechtsänderung folgt aus der DSGVO: Zur Reduzierung der Bürokratie ist das Verfahrensverzeichnis nach Artikel 30 DSGVO nur der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen (Marschall in: Roßnagel, DSGVO, § 3 Rn. 180). Das Einsichtsrecht ist nach dem bisherigen § 8 Absatz 2 DSG NRW für Verfahren nach dem VSG NRW beschränkt und gilt nach § 8 Absatz 2 S. 2 Nr. 1 DSG NRW-alt nicht, soweit die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

b) Absatz 2

Der bisherige Absatz 2 wird durch eine Neuregelung ersetzt.

Gemäß § 8 Absatz 4 VSG NRW ist geregelt, dass Unterlagen, die die nach § 8 Absatz 1 und 2 gespeicherten Angaben belegen, auch gespeichert werden dürfen, wenn in ihnen weitere personenbezogene Daten Dritter enthalten sind. Solche Belegdokumente dürfen jedoch entgegen § 12 Absatz 2-alt aufgrund verschiedener landes- und bundesrechtlicher Regelungen gerade nicht in jedem Fall übermittelt werden. § 12 Absatz 2-alt, welcher ursprünglich im Zusammenhang mit einer – später gestrichenen – Zugriffsbeschränkung von Textdateien stand, ist nicht eindeutig: Aus dem Wortlaut könnte gefolgert werden, dass Belegdateien ausnahmslos zu übermitteln sind. Zur Vermeidung einer Inkohärenz ist § 12 Absatz 2-alt daher aufzuheben.

Mit § 12 Absatz 2-neu werden datenschutzrechtliche Regelungen zur Ausgestaltung des Verfahrensverzeichnisses getroffen, die mit der Aufhebung von § 8 Absatz 1 DSG NRW-alt entfallen sind.

Nummer 1 wurde aus Artikel 30 Absatz 1 Buchstabe a. DSGVO übernommen und soll der zweifelsfreien Identifizierung des Verantwortlichen und ggf. gemeinsamen Verantwortlichen dienen. Nummer 2 bis 6 übernehmen im Wesentlichen die Regelungen in § 8 Absatz 1 Nummer 2 bis 6 DSG NRW-alt. In Nummer 7 bis 10 werden die Regelungen des § 70 Nummer 5 bis 9 BDSG übernommen. Neu ist, dass ein „Profiling“ – soweit verwendet - anzugeben ist. Der Begriff „Profiling“ ist in § 31 Absatz 2 durch Verweis auf § 46 BDSG (dort Nummer. 4) legaldefiniert. Profiling umfasst jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte einer Person zu bewerten, um zum Beispiel Interessen, Zuverlässigkeit, das Verhalten, die Aufenthaltsorte oder einen Ortswechsel der Person zu analysieren oder vorherzusagen.

Zu § 15

Mit dieser Vorschrift werden bereichsspezifisch Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit geregelt. Dies ist notwendig, da diese Befugnisse aus § 24 DSG NRW-alt wegfallen (diese bestanden im Wesentlichen aus dem Instrument der Beanstandung). Die nunmehr in Artikel 58 DSGVO in Verbindung mit § 28 Absatz 2 DSG NRW-neu geregelten Durchgriffsbefugnisse des Landesbeauftragten (darunter Letztentscheidungs-

und Anordnungsbefugnisse, z.B. Verbot der Verarbeitung, Artikel 58 Absatz 2 Buchstabe f DSGVO durch die Aufsichtsbehörde) sind mit den fachlichen Bedürfnissen der Verfassungsschutzbehörde nicht vereinbar.

a) Absatz 1

Das Recht auf Anrufung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit ergab sich bisher aus § 25 DSG NRW a.F. in Verbindung mit § 31 VSG NRW. In § 15 Absatz 1 wird die Regelung des § 26a Absatz 1 BVerfSchG-neu übernommen. Im Interesse einer Einheitlichkeit mit bundesrechtlichen Regelungen wird dabei eng dem Wortlaut des BVerfSchG gefolgt, der auf eine erfolgte Rechtsverletzung abstellt. Anerkannt ist, dass im Bereich der verdeckten Informationsverarbeitung die Darlegungsverpflichtungen für die betroffene Person bei der Rüge von Datenschutzverstößen geringer sind als im allgemeinen Datenschutzrecht.

b) Absatz 2

Das Recht bzw. die Pflicht zur Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit wird in § 15 Absatz 2 Satz 1 unter Übernahme der Formulierung des § 26a Absatz 2 Satz 1 BDSG-neu bereichsspezifisch geregelt. Bisher ergeben sich die Kontrollrechte und -pflichten der oder des Landesbeauftragten aus § 22 DSG NRW-alt in Verbindung mit § 31 VSG NRW. Im Hinblick auf die Kontrolle durch die G10-Kommission verweist § 30 Absatz 5 Satz 5 VSG NRW-alt bisher auf § 24 Absatz 2 Satz 3 des BDSG-alt. Nach § 24 Absatz 2 Satz 3 des BDSG-alt unterliegen personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des G 10 unterliegen, nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten, es sei denn, die Kommission ersucht diese bzw. diesen, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Bund hat in § 26a Absatz 2 Satz 2 BVerfSchG-neu eine Nachfolgeregelung zu § 24 Absatz 2 Satz 3 BDSG-alt geschaffen, die in § 15 Absatz 2 Satz 2 übernommen wird. Insoweit wird auf die Gesetzesbegründung zu § 26a Absatz 2 Satz 2 BVerfSchG-neu (BT-Drs. 18/11325, S. 122) Bezug genommen. Bei der Verarbeitung von personenbezogenen Daten im Rahmen von Maßnahmen mit erhöhter Eingriffsintensität können sich die Kontrollzuständigkeiten der G 10-Kommission und der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit überschneiden. Erstere ist gemäß § 30 Absatz 5 VSG NRW für die Entscheidung über die Durchführung einer Maßnahme zuständig und kann auch den weiteren Umgang mit den erhobenen personenbezogenen Daten prüfen. Soweit die Kenntnis solcher Daten für die Wahrnehmung der Kontrollaufgaben der oder des Letztgenannten erforderlich ist, soll diese oder dieser nicht von einer Kenntnisnahme der im Rahmen solcher Maßnahmen erhobenen personenbezogenen Daten ausgeschlossen sein.

c) Absatz 3

§ 15 Absatz 3 greift die Regelung in § 22 Absatz 2 Satz 2 DSG NRW-alt bereichsspezifisch auf. Die Formulierung des § 26a Absatz 3 BVerfSchG-neu wurde übernommen.

d) Absatz 4

Absatz 4 entspricht § 26a Absatz 4 BVerfSchG. Mit diesem Absatz werden auch Tätigkeiten Dritter für Aufgaben der Verfassungsschutzbehörde eingeschlossen. Es wird auf die Gesetzesbegründung zu § 26 a Absatz 4 BVerfSchG-neu (BT-Drs. 18/11325, S. 123) Bezug genommen.

e) Absatz 5

§ 15 Absatz 5 (Befugnisse der oder des Landesbeauftragten) übernimmt die bundesrechtliche Regelung des § 16 Absatz 2 BDSG-neu. Der Bund hat diese Regelung (betreffend die oder den Bundesbeauftragten für Datenschutz und Informationsfreiheit) u.a. für Datenverarbeitungen geschaffen, deren Zwecke außerhalb der DSGVO und der Richtlinie (EU) 2016/680 liegen (BT-Drs. 18/11325, S. 88). Unter Berücksichtigung der fachlichen Bedürfnisse sieht die Regelung keine Durchgriffsbefugnisse gegenüber dem Verantwortlichen vor, sondern dem Bundesbeauftragten stehen die aus § 25 BDSG-alt (bzw. im Landesrecht § 24 Absatz 1 Satz 1 Nummer 1, Absatz 2, Absatz 4 Satz 1 DSG NRW-alt) bekannte Maßnahme der Beanstandung und das aus Artikel 47 Absatz 2 Buchstabe a der Richtlinie (EU) 2016/680 entnommene Recht zur Warnung zur Verfügung. Das Recht zur Warnung gilt auch im Anwendungsbereich der DSGVO (Artikel 58 Absatz 2 Buchstabe a).

Zu § 17

a) Absatz 4 Satz 3

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinition in § 46 Nummer 3 des BDSG-neu.

b) Absatz 5 Satz 1

Es handelt sich um eine redaktionelle Änderung zur Berichtigung eines fehlerhaften Verweises.

Zu § 21 Satz 3

Die Änderung ist eine Folgeänderung der neuen Begriffsdefinition in § 46 Nummer 3 des BDSG-neu.

Zu § 30 Absatz 5

Die Änderung in Absatz 5 Satz 2 ist eine Folgeänderung zu der neuen Begriffsdefinition in § 46 Nummer 2 des BDSG-neu. Der Begriff der Verarbeitung umfasst das Erheben und das Nutzen personenbezogener Daten, so dass die letztgenannten Begriffe zu streichen sind.

Die Neufassung von § 30 Absatz 5 Satz 5 ist eine Folgeänderung aufgrund der Neufassung des § 24 Absatz 2 Satz 3 BDSG-alt in § 26a Absatz 2 Satz 2 BVerfSchG-neu sowie der Aufnahme dieser Regelung als landesspezifische Regelung in § 15 Absatz 2.

Zu § 31

a) Absatz 1

Bisher war das DSG NRW gemäß § 31 VSG NRW bei der Erfüllung der Aufgaben durch die Verfassungsschutzbehörde subsidiär anwendbar. Absatz 1 schließt nunmehr die Anwendung des novellierten DSG NRW ausdrücklich aus, da die inhaltlichen Regelungen des DSG NRW-alt mit dem 25. Mai 2018 durch die dann in vielen Rechtsbereichen unmittelbar geltende DSGVO abgelöst werden und das DSG NRW-neu dann in erster Linie Regelungen zur Durchführung der DSGVO enthält.

Die aufgrund des vollständigen Ausschlusses erforderlichen datenschutzrechtlichen Regelungen trifft das VSG NRW selbst bzw. verweist in Absatz 2 auf das Bundesrecht, so dass ein eigenes Datenschutzregime entsteht. Das VSG NRW trifft insoweit eine bereichsspezifische Vollregelung, die abschließend im Sinne des § 4 Absatz 5 DSG NRW-neu ist und im Kern den bis zum 25. Mai 2018 bestehenden Rechtsstand fortgelten lässt.

Dies ist zulässig, da der EU gemäß Artikel 4 Absatz 2 Satz 3 EUV die Rechtsetzungskompetenz für die nationale Sicherheit und damit auch für den Aufgabenbereich des Verfassungsschutzes fehlt. Dieser Status quo wird für das VSG NRW beibehalten, indem durch den vollständigen Ausschluss des DSG NRW auch dessen § 4 Absatz 6 nicht zur Anwendung kommt. Jene Norm erweitert im Übrigen den Geltungsbereich der DSGVO in NRW auch auf Bereiche, für welche der EU die Rechtsetzungskompetenz fehlt. Die in § 18 Abs. 4 DSG NRW-neu formulierten datenschutzrechtlichen Befugnisse geben solche aus dem VSG NRW wieder und haben für die Verfassungsschutzbehörde NRW nur deklaratorischen Charakter. Die Regelung knüpft im Übrigen an die Mitwirkungsaufgabe der Verfassungsschutzbehörde NRW gemäß § 3 Abs. 4 VSG NRW an.

b) Absatz 2

Absatz 2 enthält vor dem Hintergrund der Schaffung einer Vollregelung einen Verweis auf Regelungen im BDSG-neu, welche auch im besonderen Aufgabenbereich des § 3 VSG NRW angemessen sind. Im Interesse einer einheitlichen Datenschutzterminologie werden die im BDSG-neu an die DSGVO und die Richtlinie (EU) 2016/680 angepassten Begrifflichkeiten übernommen. Auf dieser Terminologie basiert auch das neue DSG NRW.
In Anlehnung an § 27 BVerfSchG-neu wird auf die folgenden Normen verwiesen:

§ 2 BDSG-neu	Begriffsbestimmungen
§ 3 BDSG-neu	allgemeine – subsidiär anwendbare – Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen
§§ 5-7 BDSG-neu	Regelungen zum behördlichen Datenschutzbeauftragten (Benennung, Stellung, Aufgaben); die vom Bundesrecht eingeräumte Möglichkeit zur Bestellung externer Datenschutzbeauftragter wird durch die Ausnahme von § 5 Absatz 4 aus der Verweisung ausgeschlossen
§ 42 BDSG-neu	Strafvorschriften
§ 46 BDSG-neu	weitere Begriffsbestimmungen
§ 51 Absatz 1-4 BDSG-neu	Regelungen für eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten
§ 52 BDSG-neu	Verarbeitung auf Weisung des Verantwortlichen
§ 53 BDSG-neu	Datengeheimnis
§ 54 BDSG-neu	Automatisierte Einzelentscheidungen
§ 62 BDSG-neu	Auftragsverarbeitung

§ 64 BDSG-neu	Anforderungen an die Sicherheit der Datenverarbeitung
§§ 65, 66 BDSG-neu	Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten
§ 83 BDSG-neu	Schadensersatz und Entschädigung
§ 84 BDSG-neu	Strafvorschriften

Begründung zu Artikel 10 Änderung des Sicherheitsüberprüfungsgesetzes Nordrhein-Westfalen

A Allgemeiner Teil

Als Ausfluss geänderten EU-Rechts und der diesbezüglichen Novellierung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) sollen die bereichsspezifischen datenschutzrechtlichen Regelungen des Sicherheitsüberprüfungsgesetzes Nordrhein-Westfalen (SÜG NRW) angepasst und zum Teil neu gefasst werden.

Mit Inkrafttreten 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 – DSGVO) am 25. Mai 2018 wird das bisherige DSG NRW in vielen Bereichen durch EU-Recht abgelöst (s. § 69 DSG NRW-neu). Die DSGVO gilt unmittelbar in den Mitgliedstaaten der Europäischen Union für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen. Nicht in dessen Anwendungsbereich fallen Tätigkeiten, welche die nationale Sicherheit betreffen, wie etwa die Datenverarbeitung im Bereich des SÜG NRW.
Das bisherige DSG NRW tritt zum 25. Mai 2018 außer Kraft. Das neue DSG NRW trifft ergänzende Regelungen zur DSGVO und dient 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. EU L 119 vom 4. Mai 2016, S. 89).

Durch Aufnahme bereichsspezifischer Regelungen und den Verweis auf das Bundesdatenschutzgesetz (BDSG) in der Fassung vom 30. Juni 2017 (BGBl. I S. 2097) in das nordrhein-westfälische SÜG wird für dessen Anwendungsbereich eine bereichsspezifische Vollregelung geschaffen, die abschließend ist und eine subsidiäre Geltung der nicht direkt anwendbaren Verordnung (EU) 2016/679 ausschließt. Ein Verweis auf das DSG NRW-neu unterbleibt, da dieses auf den Anwendungsbereich der DSGVO zugeschnitten ist und darauf bezogene Durchführungsbestimmungen und ergänzende Regelungen trifft. Es enthält kein eigenständiges Regelungswerk mehr für Bereiche, die außerhalb des Anwendungsbereichs des Unionsrechts liegen.

Da das BDSG-neu hingegen auch die Rechtsbereiche eigenständig regelt, die außerhalb des Unionsrechts liegen und daher weder der DSGVO noch der Richtlinie (EU) 2016/680 unterfallen (BT-Drs. 18/11325, S. 74), wird im Interesse eines kohärenten und anwenderfreundlichen Datenschutzrechts im Bereich des SÜG NRW auf die bundesrechtlichen Regelungen verwiesen. Damit wird einerseits eine „Zersplitterung“ der Rechtsanwendung im Bereich des SÜG

NRW durch ein Nebeneinander der DSGVO, des landesrechtlichen DSG und des Spezialrechts im SÜG NRW vermieden und andererseits eine Harmonisierung mit den datenschutzrechtlichen Regelungen des SÜG des Bundes erreicht. Mit den Verweisen auf das Bundesrecht und der Fortgeltung der bereits im SÜG NRW etablierten Vorschriften, wird der bereits geltende Rechtsstand größtenteils beibehalten.

Neue bereichsspezifische Regelungen im SÜG NRW betreffen u.a. die Datenschutzkontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit sowie die Ausgestaltung von Verfahrensverzeichnissen. Im Übrigen wird insbesondere hinsichtlich des Grundsatzes der Einwilligung und des Datengeheimnisses, der Automatisierten Einzelentscheidungen und Abrufverfahren, der Auftragsverarbeitung und der Sicherheit der Datenverarbeitung auf das neue Bundesdatenschutzgesetz verwiesen.

B Besonderer Teil

Zu § 21

Die Änderungen in der Überschrift und in Absatz 1 und 2 sind Folgeänderungen der neuen Begriffsdefinitionen zum Umgang mit personenbezogenen Daten in § 46 Nummer 2 BDSG-neu. Gemäß § 46 Nummer 2 BDSG-neu bezeichnet der Begriff „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. Der Begriff des „Verwendens“ personenbezogener Daten hat den des „Nutzens“ abgelöst.

Zu § 22

Die Änderungen in § 22 Absatz 1, 2 und 5 sind Folgeänderungen der neuen Begriffsdefinition in § 46 Nummer 2 des BDSG-neu.

Zu § 23

Die Änderungen in der Überschrift zu § 23 und in § 23 Absatz 3 Satz 2 sind Folgeänderungen der neuen Begriffsdefinition in § 46 Nummer 3 des BDSG-neu zum Umgang mit personenbezogenen Daten. Gemäß § 46 Nummer 3 ist die „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Der Begriff des „Sperrens“ von Daten wird durch die „Einschränkung der Verarbeitung“ ersetzt.

Die Änderung in § 23 Absatz 3 Satz 3 betrifft eine Folgeänderung zu der neuen Begriffsdefinition in § 46 Nummer 2 BDSG.

Zu § 28

Die Änderung in § 28 betrifft eine Folgeänderung zu der neuen Begriffsdefinition in § 46 Nummer 2 BDSG sowie redaktionelle Anpassungen an die Schreibweise im geänderten BDSG.

Zu § 32

Die Änderung in der Überschrift zu § 32 ist eine Folgeänderung der neuen Begriffsdefinition in § 46 Nummer 2 BDSG. Die Änderungen in § 32 Satz 1 und 2 sind redaktionelle Anpassungen an die Schreibweise im geänderten BDSG und zur neuen Begriffsdefinition in § 46 Nummer 3.

Zu § 34

§ 34 enthält Anpassungen der Begrifflichkeiten im Hinblick auf den Organisationserlass vom 13. Juli 2017 (GV. NRW. S. 699). In dessen Ziff. 2 wird die Bezeichnung der obersten Landesbehörden neu gefasst.

Zu § 34a

a) Absatz 1

§ 34a trifft eine Folgeregelung aufgrund der Neufassungen des BDSG und des DSG NRW. Bisher war das DSG NRW gemäß § 2 Absatz 1 Satz 1 und Absatz 3 DSG NRW bei der Datenverarbeitung durch öffentliche Stellen des Landes subsidiär anwendbar. Absatz 1 schließt nunmehr die Anwendung des novellierten DSG NRW ausdrücklich aus, da die inhaltlichen Regelungen des DSG NRW-alt mit dem 25. Mai 2018 durch die dann in vielen Rechtsbereichen unmittelbar geltende DSGVO abgelöst werden und das DSG NRW-neu dann in erster Linie Regelungen zur Durchführung der DSGVO enthält.

Die aufgrund des vollständigen Ausschlusses erforderlichen datenschutzrechtlichen Regelungen trifft das SÜG NRW selbst bzw. verweist in Absatz 2 auf das Bundesrecht, so dass ein eigenes Datenschutzregime entsteht. Das SÜG NRW trifft insoweit eine bereichsspezifische Vollregelung, die abschließend im Sinne des § 4 Absatz 5 DSG NRW-neu ist und im Kern den bis zum 25. Mai 2018 bestehenden Rechtsstand fortgelten lässt.

Dies ist zulässig, da der EU gemäß Artikel 4 Absatz 2 Satz 3 EUV die Rechtsetzungskompetenz für die nationale Sicherheit und damit auch den Bereich der Sicherheitsüberprüfung fehlt. Dieser Status quo wird für das SÜG NRW beibehalten, indem durch den vollständigen Ausschluss des DSG NRW auch dessen § 4 Absatz 6 nicht zur Anwendung kommt. Jene Norm erweitert im Übrigen den Geltungsbereich der DSGVO in Nordrhein-Westfalen auch auf Bereiche, für welche der EU die Rechtsetzungskompetenz fehlt.

b) Absatz 2

Absatz 2 enthält vor dem Hintergrund der Schaffung einer Vollregelung einen Verweis auf Regelungen im BDSG-neu, welche auch im besonderen Aufgabenbereich des Sicherheitsüberprüfungsgesetzes NRW angemessen sind. Im Interesse einer einheitlichen Datenschutzterminologie werden die im BDSG-neu an die DSGVO und die Richtlinie (EU) 2016/680 angepassten Begrifflichkeiten übernommen. Auf dieser Terminologie basiert auch das neue DSG NRW.

In Anlehnung an § 36 Absatz 1 des Sicherheitsüberprüfungsgesetzes des Bundes vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch Artikel 5 des Gesetzes vom 30 Juni 2017 (BGBl. I 2097) geändert worden ist, wird auf die folgenden Normen verwiesen:

§ 2 BDSG-neu	Begriffsbestimmungen, insbesondere Abgrenzung von „öffentlichen Stellen“ und „nichtöffentlichen Stellen“
§ 3 BDSG-neu	allgemeine – subsidiär anwendbare – Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen
§§ 5-7 BDSG-neu	Regelungen zum behördlichen Datenschutzbeauftragten (Benennung, Stellung, Aufgaben)
§ 42 BDSG-neu	Strafvorschriften
§ 46 BDSG-neu	weitere Begriffsbestimmungen
§ 51 Absatz 1 und 3 BDSG-neu	Regelungen für eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten
§ 52 BDSG-neu	Verarbeitung auf Weisung des Verantwortlichen
§ 53 BDSG-neu	Datengeheimnis
§ 54 BDSG-neu	Automatisierte Einzelentscheidungen
§ 62 BDSG-neu	Auftragsverarbeitung
§ 64 BDSG-neu	Anforderungen an die Sicherheit der Datenverarbeitung
§§ 65, 66 BDSG-neu	Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten
§ 83 BDSG-neu	Schadensersatz und Entschädigung

Zu § 34b

Zuständige Stellen für die Sicherheitsüberprüfung im Sinne des § 1 Absatz 1 SÜG NRW-alt sind auch nichtöffentliche Stellen (z.B. politische Parteien nach Artikel 21 des GG, s. § 4 Absatz 1 Ziff. 2 SÜG NRW-alt). Die bislang geltenden Regelungen des BDSG-alt betreffend die Datenverarbeitung durch nichtöffentliche Stellen werden mit dem Inkrafttreten des BDSG-neu durch die darin enthaltenen Regelungen ersetzt.

Zu diesen Regelungen werden Ausschlüsse festgelegt, soweit im SÜG bereichsspezifische Spezialregelungen enthalten sind. Ausgeschlossen wird z.B. die Anwendung von § 16 BDSG, da in § 34c eine bereichsspezifische Regelung zur Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit getroffen wird. Klarstellend werden § 1 Absatz 8 und § 85 BDSG von der Anwendung ausgenommen, da das SÜG ein bereichsspezifisches Datenschutzvollsystem für den Bereich der Sicherheitsüberprüfungen bildet, das keinen Raum für die Anwendung des Teil 2 des BDSG oder der DSGVO bzw. der Richtlinie (EU) 2016/680 belässt.

Zu § 34c

Mit dieser Vorschrift werden bereichsspezifisch Befugnisse der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit geregelt. Dies ist notwendig, da die Befugnisse des Datenschutzbeauftragten in § 24 DSG NRW-alt entfallen. Die nunmehr in Artikel 58 der DSGVO i.V.m. § 26 Absatz 2 DSG NRW-neu geregelten Durchgriffsbefugnisse der oder des Landesbeauftragten (darunter Letztentscheidungs- und Anordnungsbefugnisse, z.B. Verbot der Verarbeitung, Artikel 58 Absatz 2 Buchstabe f. der DSGVO durch die Aufsichtsbehörde) sind mit den fachlichen Bedürfnissen im Bereich der Sicherheitsüberprüfung nicht vereinbar.

Das Recht auf Anrufung der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit ergab sich bisher aus § 25 DSG NRW für den öffentlichen Bereich. In § 34c Absatz 1 wird die Regelung des § 36a Absatz 1 SÜG-neu (Bund). übernommen und die oder der Landesbeauftrage für Datenschutz und Informationsfreiheit für zuständig erklärt. § 34c Absatz 2 regelt die Kontrollbefugnisse der oder des Landesbeauftragten. Dazu wurde die Regelung des § 36a Absatz 2 SÜG-neu übernommen. Die Kontrollbefugnisse der oder des Landesbeauftragten erstrecken sich auf öffentliche und nichtöffentliche Stellen. Im Hinblick auf die Zuständigkeitsabgrenzung zur G 10-Kommission wird auf die Gesetzesbegründung zu § 36a Absatz 2 SÜG-neu (BT-Drs. 18/11325 S. 127) Bezug genommen. Bei der Verarbeitung von personenbezogenen Daten im Rahmen von Maßnahmen mit erhöhter Eingriffsintensität können sich die Kontrollzuständigkeiten der G 10-Kommission und der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit überschneiden. Erstere ist gemäß § 30 Absatz 5 Verfassungsschutzgesetz NRW für die Entscheidung über die Durchführung einer Maßnahme zuständig und kann auch den weiteren Umgang mit den erhobenen personenbezogenen Daten prüfen. Soweit die Kenntnis solcher Daten für die Wahrnehmung der Kontrollaufgaben der oder des Letztgenannten erforderlich ist, soll diese oder dieser nicht von einer Kenntnisnahme der im Rahmen solcher Maßnahmen erhobenen personenbezogenen Daten ausgeschlossen sein.

§ 34c Absatz 4 übernimmt die bundesrechtliche Regelung des § 16 Absatz 2 BDSG-neu. Der Bund hat diese Regelung (betreffend die oder den Bundesbeauftragten für Datenschutz und Informationsfreiheit) u.a. für Datenverarbeitungen geschaffen, deren Zwecke außerhalb der DSGVO und der Richtlinie (EU) 2016/680 liegen (BT-Drs. 18/11325 S. 88). Unter Berücksichtigung der fachlichen Bedürfnisse sieht die Regelung keine Durchgriffsbefugnisse gegenüber dem Verantwortlichen vor, sondern der oder dem Bundesbeauftragten stehen die aus § 25 BDSG-alt (bzw. im Landesrecht § 24 Absatz 1 Satz 1Nummer 1, Absatz 2, Absatz 4 Satz 1 DSG NRW-alt) bekannte Maßnahme der Beanstandung und das aus Artikel 47 Absatz 2 Buchstabe a der Richtlinie (EU) 2016/680 entnommene Recht zur Warnung zur Verfügung. Das Recht zur Warnung gilt auch im Anwendungsbereich der DSGVO (Artikel 58 Absatz 2 Buchstabe a).

Zu § 34d

c) Absatz 1

§ 34d enthält Regelungen zum Führen eines für die oder den behördlichen Datenschutzbeauftragten bestimmten Verfahrensverzeichnisses. Im Anwendungsbereich des DSG NRW-alt ergab sich dies bisher aus § 8 DSG NRW. Wie bereits bisher, bezieht sich das Verfahrensverzeichnis nur auf die automatisierte Verarbeitung personenbezogener Daten.

Anders als im bisherigen § 8 DSG NRW-alt sieht § 34d kein grundsätzliches Einsichtsrecht für jedermann vor. Diese Rechtsänderung folgt aus der DSGVO: Zur Reduzierung der Bürokratie ist das Verfahrensverzeichnis nach Artikel 30 DSGVO ausschließlich der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen (Marschall in Roßnagel DSGVO § 3 Rn. 180).

d) Absatz 2

Nummer 1 wurde aus Artikel 30 Absatz 1 Buchstabe a DSGVO übernommen und soll der zweifelsfreien Identifizierung des Verantwortlichen und ggf. gemeinsamen Verantwortlichen dienen. Nr. 2 bis 6 übernehmen im Wesentlichen die Regelungen in § 8 Absatz 1 Nummer 2 bis 6 DSG NRW-alt. In Nummer 7 bis 10 werden die Regelungen des § 70 Nummer 5 bis 9 BDSG übernommen. Neu ist, dass ein „Profiling“ – soweit verwendet - anzugeben ist. Der Begriff „Profiling“ ist in § 31 Absatz 2 durch Verweis auf § 46 BDSG (dort Nummer 4) legaldefiniert. Profiling umfasst jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte einer Person zu bewerten, um zum Beispiel Interessen, Zuverlässigkeit, das Verhalten, die Aufenthaltsorte oder einen Ortswechsel der Person zu analysieren oder vorherzusagen.