



Landesbeauftragte
für Datenschutz
und Akteneinsicht

Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz

Brandenburgisches Polizei-, Justizvollzugs-
und Maßregelvollzugsdatenschutzgesetz
BbgPJMDSG
Justizvollzugs-
Brandenburgisches Po
etz BbgPJMDSG
ollzugsdatensch
ollzugs- un
nes Po
cz BbgPJMDSG
gesetz

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de
Internet: <https://www.LDA.Brandenburg.de>

Stand: 1. Auflage, November 2019

Druck: KUSS Kopierservice GmbH

Brandenburgisches Polizei-,
Justizvollzugs- und
Maßregelvollzugsdaten-
schutzgesetz
(BbgPJMDSG)

Vorwort	7
----------------------	----------

Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz

Abschnitt 1

Allgemeine Bestimmungen und Grundsätze

§ 1	Anwendungsbereich	9
§ 2	Begriffsbestimmungen	10
§ 3	Grundsätze der Datenverarbeitung	15
§ 4	Unterscheidung zwischen Tatsachen und Beurteilungen	16

Abschnitt 2

Allgemeine Bestimmungen für die Verarbeitung personenbezogener Daten

§ 5	Allgemeine Angaben zur Verarbeitung personenbezogener Daten	16
§ 6	Erhebung personenbezogener Daten	17
§ 7	Hinweispflichten zur Erhebung personenbezogener Daten mit Kenntnis der betroffenen Person	17
§ 8	Unterrichtungspflicht nach Erhebung personenbezogener Daten ohne Kenntnis der betroffenen Person	18
§ 9	Verarbeitung personenbezogener Daten besonderer Kategorien	18
§ 10	Einwilligung	19
§ 11	Zweckänderung	19
§ 12	Weiterverarbeitung zu statistischen und wissenschaftlichen Zwecken sowie zur Aus- und Fortbildung	20
§ 13	Übermittlung	20
§ 14	Berichtigung	21
§ 15	Löschung	22
§ 16	Automatisierte Entscheidung im Einzelfall	23

Abschnitt 3

Technische und organisatorische Anforderungen an die Datenverarbeitung, Dokumentation

§ 17	Technische und organisatorische Maßnahmen	24
§ 18	Vertrauliche Meldung von Verstößen	24
§ 19	Datenschutz durch Gestaltung von Technik und datenschutzfreundliche Voreinstellungen	24
§ 20	Sicherheit der Datenverarbeitung	25
§ 21	Datenschutz-Folgenabschätzung	26
§ 22	Zusammenarbeit mit der oder dem Landesbeauftragten	27
§ 23	Anhörung der oder des Landesbeauftragten	27
§ 24	Verzeichnis der Verarbeitungstätigkeiten	29
§ 25	Protokollierung	30

Abschnitt 4

An der Datenverarbeitung Beteiligte

§ 26	Datengeheimnis	32
§ 27	Datenverarbeitung im Auftrag	32
§ 28	Gemeinsam Verantwortliche	34

Abschnitt 5

Verletzung der Sicherheit personenbezogener Daten

§ 29	Meldung an die Landesbeauftragte oder den Landesbeauftragten	35
§ 30	Unterrichtung der betroffenen Person	36

Abschnitt 6

Behördliche Datenschutzbeauftragte

§ 31	Bestellung	37
§ 32	Stellung und Rechte	37
§ 33	Aufgaben	38

Abschnitt 7

Datenschutzrechtliche Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten

§ 34	Aufgaben	39
§ 35	Unterstützung durch Verantwortliche und Auftragsverarbeiter	41
§ 36	Befugnisse	42
§ 37	Tätigkeitsbericht	43
§ 38	Zusammenarbeit zur einheitlichen Umsetzung der Richtlinie (EU) 2016/680	43

Abschnitt 8

Rechte der betroffenen Person

§ 39	Verfahren für die Ausübung der Rechte der betroffenen Person	44
§ 40	Recht auf Auskunft	44
§ 41	Recht auf Berichtigung und Löschung	46
§ 42	Recht auf Beschwerde	47
§ 43	Schadensersatz	47

Abschnitt 9

Gerichtlicher Rechtsschutz und Schlussvorschriften

§ 44	Gerichtlicher Rechtsschutz	48
§ 45	Einschränkung eines Grundrechts	48
§ 46	Übergangsregelung	49

Vorwort

Seit dem 25. Mai 2018 gilt in allen Mitgliedstaaten der Europäischen Union die Datenschutz-Grundverordnung. Sie regelt den Datenschutz EU-weit einheitlich für viele Aspekte unseres Lebens. Davon ausgenommen sind einzelne Bereiche, für die wegen ihrer besonderen Herausforderungen spezielle Regelungen geschaffen werden müssen. Dies betrifft die Verarbeitung personenbezogener Daten für Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten und Ordnungswidrigkeiten – einschließlich der Abwehr von Gefahren für die öffentliche Sicherheit – sowie für den Zweck der Strafvollstreckung. Für diese Aufgaben hat die EU – zeitlich parallel zur Datenschutz-Grundverordnung – die Richtlinie (EU) 2016/680 für die Bereiche Justiz und Inneres erlassen, die – anders als die Datenschutz-Grundverordnung – nicht unmittelbar gilt, sondern erst von den Mitgliedstaaten jeweils durch Gesetze in nationales Recht überführt werden muss. Auf diese Weise werden den Mitgliedstaaten für die Gefahrenabwehr, die Strafverfolgung und den Strafvollzug größere Handlungsspielräume eröffnet.

Das im Folgenden abgedruckte Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ist das für Brandenburg wesentliche Regelwerk zur Umsetzung der Richtlinie (EU) 2016/680. Es gilt für die Polizei, den Justizvollzug und den Maßregelvollzug des Landes und regelt für die genannten drei Bereiche den Umgang mit persönlichen Daten, soweit deren Verarbeitung für die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten und Ordnungswidrigkeiten, für die Gefahrenabwehr sowie für die Strafvollstreckung erforderlich ist. Verarbeiten Polizei, Justiz- und Maßregelvollzug dagegen personenbezogene Daten zu anderen Zwecken, wie beispielsweise für die Personalverwaltung, oder übermitteln sie Daten für andere Zwecke als diejenigen der Richtlinie (EU) 2016/680, etwa an Sozialleistungsträger oder Ausländerbehörden, haben auch sie die Datenschutz-Grundverordnung zu beachten.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist auch für die Datenverarbeitung nach dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz und die Einhaltung seiner Regelungen durch die Landesbehörden die zuständige Aufsichtsbehörde. Sie ist bei der

Ausübung ihrer Befugnisse unabhängig, verfügt aber im Vergleich zur Datenschutz-Grundverordnung nur über eingeschränkte Abhilfemöglichkeiten. Bei Verstößen gegen das Gesetz kann sie zwar Warnungen und Beanstandungen aussprechen. Das Recht, Behörden zu einem bestimmten Handeln anzuweisen, wie etwa dazu, einem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, hat sie aber nur bei erheblichen Verstößen und auch nur, wenn die Behörde trotz vorheriger Warnung oder Beanstandung keine Abhilfe geschaffen hat.

Auffällige Unterschiede zwischen der Datenschutz-Grundverordnung und dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz finden sich außerdem im Bereich der Rechte der Bürgerinnen und Bürger. Bedingt durch die Besonderheiten der Aufgaben von Polizei sowie Straf- und Maßregelvollzug sind diese weniger weitgehend.

Ob sich das Gesetz bewährt und dem Datenschutz ausreichenden Raum gibt, wird sich in der Praxis erweisen.



Dagmar Hartge
Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht

Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für die Verarbeitung personenbezogener Daten durch die Polizei sowie den Justiz- und Maßregelvollzug des Landes Brandenburg

(Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz – BbgPJMDSG)

vom 19. Juni 2019 (GVBl. I Nr. 43)

Abschnitt 1

Allgemeine Bestimmungen und Grundsätze

§ 1 Anwendungsbereich

(1) Dieses Gesetz regelt die Verarbeitung personenbezogener Daten in Dateisystemen zum Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten und der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit durch

1. die Polizei, auch für die Abwehr von Gefahren für die öffentliche Ordnung sowie für die Verfolgung und Ahndung von Ordnungswidrigkeiten und
2. die Justizvollzugs- und Maßregelvollzugsbehörden für vollzugliche Zwecke.

(2) Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben nach Absatz 1 wahr, richtet sich auch deren Verarbeitung personenbezogener Daten nach diesem Gesetz. Für Auftragsverarbeiter der in den Absatz 1 genannten öffentlichen Stellen gilt dieses Gesetz nur,

soweit sich die Bestimmungen ausdrücklich an Auftragsverarbeiter richten.

(3) Mit Ausnahme der §§ 18 Absatz 4, 32 und 33 des Brandenburgischen Datenschutzgesetzes findet das Brandenburgische Datenschutzgesetz keine Anwendung.

§ 2 Begriffsbestimmungen

Dieses Gesetz bestimmt die nachstehenden Begriffe wie folgt:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als „identifizierbar“ wird eine 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, von anderen Personen unterschieden werden kann;
2. „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. „Automatisiert“ ist eine Datenverarbeitung, wenn sie durch den Einsatz eines gesteuerten technischen Verfahrens selbstständig ablaufen kann. Insbesondere ist
 - a) „Erheben“ (Erhebung) das Beschaffen personenbezogener Daten über die betroffene Person,
 - b) „Berichtigen“ (Berichtigung) die Herbeiführung des der Wirklichkeit entsprechenden Aussagegehalts der personenbezogenen Daten im Hinblick auf den Zeitpunkt, auf den sich die Daten beziehen, insbesondere durch Ersetzung oder Veränderung,
 - c) „Verändern“ (Veränderung) das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

- d) „Löschen“ (Löschung) das Unkenntlichmachen der auf einem elektronischen Datenträger gespeicherten personenbezogenen Daten beziehungsweise die Zerstörung (Vernichtung) eines physischen Datenträgers,
 - e) „Einschränken der Verarbeitung“ (Einschränkung) die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung zu verhindern,
 - f) „Speichern“ (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke der weiteren Verarbeitung,
 - g) „Offenlegen“ (Offenlegung) jede Bereitstellung personenbezogener Daten zur Kenntnisnahme, insbesondere durch „Übermitteln“ (Übermittlung), das heißt das Bekanntgeben personenbezogener Daten an Dritte in der Weise, dass die personenbezogenen Daten an Dritte weitergegeben werden oder Dritte zur Einsicht oder zum Abruf bereitgehaltene personenbezogene Daten einsehen oder abrufen,
 - h) „Abfragen“ (Abfrage) der automatisierte Zugriff auf personenbezogene Daten,
 - i) „Nutzen“ (Nutzung) jede sonstige Verwendung personenbezogener Daten durch den Verantwortlichen zur Erfüllung seiner Aufgaben;
3. „Pseudonymisieren“ (Pseudonymisierung) die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die dies gewährleisten;
4. „Anonymisieren“ (Anonymisierung) das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer betroffenen Person zugeordnet werden können;

5. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine betroffene Person beziehen, zu bewerten, insbesondere um Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser betroffenen Person zu analysieren oder vorherzusagen;
6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird oder ob sie automatisiert oder nichtautomatisiert erfolgt. Darunter fallen auch sonstige dienstlichen Zwecken dienende Unterlagen (Akten), soweit es sich nicht um Vorentwürfe und Notizen handelt, die nicht Bestandteil eines Vorgangs sind und alsbald vernichtet werden sollen;
7. „Verantwortlicher“ eine öffentliche Stelle im Sinne von Nummer 20 Buchstabe b und d, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten nach § 1 entscheidet;
8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
9. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, mit Ausnahme der betroffenen Person, des Verantwortlichen, des Auftragsverarbeiters und der Personen, die aufgrund einer Weisung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten;
10. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten

durch die genannten öffentlichen Stellen erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

11. „Drittstaat“ jeder Staat, der weder Mitglied in der Europäischen Union ist noch die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwendet und den Mitgliedstaaten der Europäischen Union insoweit gleichsteht (Schengen-assoziiertes Staat);
12. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;
13. „Verletzung der Sicherheit personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unbefugten Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;
14. „personenbezogene Daten besonderer Kategorien“
 - a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen 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;
15. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer betroffenen Person, die eindeutige Informationen über die Physiologie oder

die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;

16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer betroffenen Person, die die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;
17. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer betroffenen Person, einschließlich Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
18. „die oder der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht“ (die oder der Landesbeauftragte) die vom Land Brandenburg nach §§ 14 ff. des Brandenburgischen Datenschutzgesetzes errichtete, unabhängige und für die Überwachung der Einhaltung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zuständige Aufsichtsbehörde nach Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680;
19. „Einwilligung“ jede in Kenntnis der Rechtsfolgen für einen bestimmten Fall, freiwillig 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“
 - a) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und der Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform,
 - b) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, ei-

ner Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform,

- c) die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Mitgliedstaates der Europäischen Union sowie die nach Teil 3 Titel V Kapitel 4 und 5 des Vertrages über die Arbeitsweise der Europäischen Union errichteten Agenturen, Einrichtungen und sonstigen Stellen und
 - d) nichtöffentliche Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen;
21. „nichtöffentliche Stellen“ natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter Nummer 20 Buchstabe d fallen.

§ 3 Grundsätze der Datenverarbeitung

Personenbezogene Daten

1. müssen auf rechtmäßige Weise (Grundsatz der Rechtmäßigkeit) und nach Treu und Glauben verarbeitet werden,
2. dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und in einer mit diesen Zwecken zu vereinbarenden Weise verarbeitet werden (Grundsatz der Zweckbindung),
3. sind auf das für die Zwecke der Verarbeitung erforderliche Maß zu beschränken (Grundsatz der Datenminimierung),
4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Grundsatz der Richtigkeit),
5. dürfen nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht, wie es für die

in § 1 Absatz 1 genannten Zwecke erforderlich ist (Grundsatz der Speicherbegrenzung) und

6. sind auf eine Weise zu verarbeiten, die die Sicherheit der Daten gewährleistet; sie müssen durch geeignete technische und organisatorische Maßnahmen insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sein (Grundsatz der Integrität und Vertraulichkeit).

§ 4 Unterscheidung zwischen Tatsachen und Beurteilungen

Bei der Verarbeitung ist soweit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen.

Abschnitt 2

Allgemeine Bestimmungen für die Verarbeitung personenbezogener Daten

§ 5 Allgemeine Angaben zur Verarbeitung personenbezogener Daten

Der Verantwortliche veröffentlicht

1. seinen Namen und seine Erreichbarkeit,
2. die Erreichbarkeit der oder des behördlichen Datenschutzbeauftragten,
3. eine Beschreibung der Zwecke, zu denen er personenbezogene Daten verarbeitet,
4. allgemeine Hinweise zu den Rechten der betroffenen Person auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung sowie auf Beschwerde bei der oder dem Landesbeauftragten und

5. den Namen und die Erreichbarkeit der oder des Landesbeauftragten.

§ 6 Erhebung personenbezogener Daten

(1) Personenbezogene Daten sind grundsätzlich bei der betroffenen Person mit deren Kenntnis oder aus allgemein zugänglichen Quellen zu erheben.

(2) Im Justiz- und Maßregelvollzug ist eine Erhebung personenbezogener Daten ohne Kenntnis der betroffenen Person für vollzugliche Zwecke nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden.

(3) Die Polizei darf personenbezogene Daten ohne Kenntnis der betroffenen Person nur in den durch das Brandenburgische Polizeigesetz bestimmten Fällen erheben.

§ 7 Hinweispflichten zur Erhebung personenbezogener Daten mit Kenntnis der betroffenen Person

(1) Erhebt der Verantwortliche personenbezogene Daten bei der betroffenen Person mit deren Kenntnis, teilt er ihr den Zweck und die Rechtsgrundlage der Datenerhebung sowie den Empfänger der Daten mit und weist sie auf ihre Rechte auf Auskunft, Berichtigung und Löschung nach den §§ 40 und 41 hin. Soweit die betroffene Person bereits über die nach Satz 1 erforderlichen Informationen verfügt, insbesondere in den Fällen einer wiederholten oder fortlaufenden Datenerhebung, kann die Mitteilung unterbleiben.

(2) Soweit die betroffene Person zu einer Auskunft verpflichtet ist oder ihre Angaben Voraussetzung für die Gewährung von Rechtsvorteilen sind, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben, hinzuweisen.

(3) Sind die Angaben für die Gewährung einer Leistung erforderlich, ist die betroffene Person über die möglichen Folgen einer Nichtbeantwortung zu belehren.

§ 8 Unterrichtungspflicht nach Erhebung personenbezogener Daten ohne Kenntnis der betroffenen Person

(1) Der Verantwortliche unterrichtet die betroffene Person, soweit dies gesetzlich vorgesehen ist, über eine ohne ihre Kenntnis vorgenommene Erhebung personenbezogener Daten unter Angabe dieser Daten sowie zumindest über

1. die Rechtsgrundlage und den Zweck der Erhebung,
2. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer und
3. den Empfänger der personenbezogenen Daten.

(2) Soweit gesetzlich nicht Abweichendes bestimmt ist, darf der Verantwortliche die Unterrichtung nach Absatz 1 aufschieben, einschränken oder unterlassen, solange und soweit andernfalls die Erreichung eines in § 1 genannten Zwecks oder Rechtsgüter gefährdet würden und das Interesse an der Vermeidung dieser Gefahren das Interesse der betroffenen Person an der Unterrichtung überwiegt.

§ 9 Verarbeitung personenbezogener Daten besonderer Kategorien

(1) Die Verarbeitung personenbezogener Daten besonderer Kategorien ist nur zulässig, soweit sie für die Aufgabenerfüllung des Verantwortlichen zu den in § 1 Absatz 1 genannten Zwecken gesetzlich vorgesehen und unerlässlich ist.

(2) Die an der Verarbeitung personenbezogener Daten besonderer Kategorien Beteiligten sind auf die besondere Schutzbedürftigkeit dieser Daten hinzuweisen. Der Verantwortliche beschränkt den Zugriff auf personenbezogene Daten besonderer Kategorien auf die Bediensteten, für deren Tätigkeiten die Verarbeitung dieser Daten unerlässlich ist.

§ 10 Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung erfolgen kann, insbesondere wenn dies in einer Rechtsvorschrift vorgesehen ist, hat der Verantwortliche die Einwilligung der betroffenen Person nachzuweisen.

(2) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, sind deren Umstände, etwa die besondere Situation der Freiheitsentziehung oder der polizeilichen Vernehmung, zu berücksichtigen.

(3) Soweit personenbezogene Daten besonderer Kategorien verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

(4) Das Ersuchen um Einwilligung erfolgt in einer verständlichen, klaren und einfachen Sprache. Beinhaltet die schriftliche Erklärung der Einwilligung noch andere Sachverhalte, so muss sie von diesen klar zu unterscheiden sein.

(5) Die betroffene Person ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Zweck der Verarbeitung ihrer personenbezogenen Daten, bei einer beabsichtigten Übermittlung über die Empfänger sowie den Zweck der Übermittlung aufzuklären; sie ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

§ 11 Zweckänderung

(1) Der Verantwortliche darf personenbezogene Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, verarbeiten, wenn der andere Zweck im jeweiligen Anwendungsbereich dieses Gesetzes liegt, der Verantwortliche befugt ist, Daten auch zu diesem Zweck zu verarbeiten und die Datenverarbeitung erforderlich und verhältnismäßig ist.

(2) Die Verarbeitung personenbezogener Daten zu einem anderen, nicht in den jeweiligen Anwendungsbereich dieses Gesetzes fallen-

den Zweck ist nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich vorsieht.

(3) Personenbezogene Daten, die zu einem der in § 1 Absatz 1 genannten Zwecke erhoben wurden, dürfen auch zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen verarbeitet werden. Satz 1 gilt im Justiz- und Maßregelvollzug auch für Zwecke des gerichtlichen Rechtsschutzes und des Schutzes der Gesundheit der Gefangenen und Untergebrachten.

§ 12 Weiterverarbeitung zu statistischen und wissenschaftlichen Zwecken sowie zur Aus- und Fortbildung

(1) Der Verantwortliche kann personenbezogene Daten zu statistischen Zwecken nutzen. Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

(2) Für die Weiterverarbeitung personenbezogener Daten für wissenschaftliche Zwecke, auch durch den Verantwortlichen, gilt § 476 der Strafprozessordnung entsprechend mit der Maßgabe, dass auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können. Die Übermittlung kann auch auf elektronischem Wege erfolgen. Die Rechte auf Auskunft nach § 40 und auf Berichtigung oder Löschung nach § 41 bestehen nicht, soweit die Wahrnehmung eines dieser Rechte die Erreichung der wissenschaftlichen Zwecke unmöglich machen oder ernsthaft beeinträchtigen oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Der Verantwortliche darf zuvor anonymisierte personenbezogene Daten zur Aus- und Fortbildung nutzen. Zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verarbeitet werden.

§ 13 Übermittlung

(1) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Der Verantwortliche dokumentiert die Übermittlung und deren Gründe.

(2) Der Empfänger darf die übermittelten personenbezogenen Daten nur zu dem Zweck verarbeiten, zu dem sie übermittelt worden sind, soweit gesetzlich nichts anderes bestimmt ist. Der Verantwortliche hat Empfänger außerhalb des öffentlichen Bereichs sowie in Drittstaaten und internationalen Organisationen bei der Datenübermittlung auf diese Zweckbindung hinzuweisen. Bestehen darüber hinausgehende Verarbeitungsbeschränkungen, etwa im Hinblick auf personenbezogene Daten besonderer Kategorien, sind Empfänger auch darauf hinzuweisen.

(3) Soweit dies mit angemessenem Aufwand möglich ist, sind die personenbezogenen Daten vor ihrer Übermittlung oder sonstigen Offenlegung auf Richtigkeit, Vollständigkeit und Aktualität zu überprüfen. Der Verantwortliche macht bei der Übermittlung personenbezogener Daten nach Möglichkeit Angaben, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Aktualität der personenbezogenen Daten zu beurteilen.

(4) Stellt der Verantwortliche fest, dass er unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt hat, so teilt er dies dem Empfänger unverzüglich mit und gibt ihm erforderlichenfalls auf, die betreffenden Daten zu löschen, zu berichtigen oder ihre Verarbeitung einzuschränken.

(5) Personenbezogene Daten, die an nichtöffentliche Stellen übermittelt werden sollen, sind vor der Übermittlung wenigstens zu pseudonymisieren, soweit die Identität der betroffenen Person zur Erreichung des Zwecks der Übermittlung nicht erforderlich ist.

(6) Für Übermittlungen an Drittstaaten und an internationale Organisationen gelten die §§ 78 bis 81 des Bundesdatenschutzgesetzes entsprechend.

§ 14 Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig, unvollständig oder nicht mehr aktuell sind. Soweit dies mit angemessenem Aufwand möglich ist, sind personenbezogene Daten vor ihrer Verarbeitung auf Richtigkeit, Vollständigkeit und Aktualität zu überprüfen. In Akten genügt es, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt oder aus welchem Grund sie unrichtig

waren oder unrichtig geworden sind. Eine Vervollständigung personenbezogener Daten kann auch mittels einer ergänzenden Erklärung erfolgen.

(2) Die Pflicht zur Berichtigung nach Absatz 1 Satz 1 betrifft nicht den Inhalt von Zeugenaussagen und gutachtlichen Stellungnahmen.

(3) Kann die Richtigkeit oder Unrichtigkeit personenbezogener Daten nicht festgestellt werden, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. Eine Verarbeitung dieser Daten darf nur erfolgen, um deren Richtigkeit oder Unrichtigkeit festzustellen.

(4) Hat der Verantwortliche von einer anderen Stelle unrichtige Daten empfangen, setzt er die übermittelnde Stelle unverzüglich hierüber und über die Berichtigung oder die Einschränkung der Verarbeitung in Kenntnis.

§ 15 Löschung

(1) Der Verantwortliche löscht personenbezogene Daten unverzüglich, wenn ihre Verarbeitung nicht zulässig oder nicht mehr erforderlich ist.

(2) Der Verantwortliche legt Fristen zur Prüfung der Erforderlichkeit der weiteren Speicherung fest. Dabei sind der Zweck der Speicherung sowie die Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Die Fristen beginnen

1. bei der Polizei mit dem Tag der Speicherung und
2. im Justiz- und Maßregelvollzug mit der Verlegung oder der Entlassung der betroffenen Person aus der Justizvollzugsanstalt oder der Einrichtung des Maßregelvollzuges.

(3) An die Stelle der Löschung tritt die Einschränkung der Verarbeitung, wenn

1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen betroffener Personen beeinträchtigt werden oder

2. dies erforderlich ist

- a) zur Feststellung, Durchsetzung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Erfüllung der Aufgaben nach § 1,
- b) zu Zwecken der Datensicherung oder Datenschutzkontrolle oder
- c) zu sonstigen Beweis Zwecken.

Im Fall von Satz 1 Nummer 1 dürfen die Daten nur mit schriftlicher Einwilligung der betroffenen Person verwendet werden. In den anderen Fällen dürfen die Daten nur für den Zweck der Einschränkung verwendet werden. Die Gründe für die Einschränkung der Verarbeitung werden dokumentiert.

§ 16 Automatisierte Entscheidung im Einzelfall

(1) Eine ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist

- 1. im Justiz- und Maßregelvollzug unzulässig,
- 2. für polizeiliche Zwecke nach § 1 Absatz 1 Nummer 1 nur aufgrund einer Rechtsvorschrift zulässig, die sicherstellt, dass der Verantwortliche jederzeit in das automatisierte Verfahren eingreifen kann.

(2) Entscheidungen nach Absatz 1 Nummer 2 dürfen nicht auf personenbezogenen Daten besonderer Kategorien beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Profiling, das zur Folge hat, dass die betroffene Person auf der Grundlage von personenbezogenen Daten besonderer Kategorien diskriminiert wird, ist verboten.

Abschnitt 3

Technische und organisatorische Anforderungen an die Datenverarbeitung, Dokumentation

§ 17 Technische und organisatorische Maßnahmen

(1) Der Verantwortliche stellt durch technische und organisatorische Maßnahmen sicher, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit diesem Gesetz erfolgt.

(2) Bei der Auswahl der Maßnahmen nach Absatz 1 sind die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung, die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechtsgüter der betroffenen Personen sowie der jeweilige Stand der Technik und die Kosten der Einrichtung und Durchführung zu berücksichtigen. Dies gilt insbesondere für die Verarbeitung personenbezogener Daten besonderer Kategorien. Der Verantwortliche dokumentiert die Risikoabwägung nach Satz 1.

(3) Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

§ 18 Vertrauliche Meldung von Verstößen

Der Verantwortliche ermöglicht die vertrauliche Mitteilung von Verstößen gegen die zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften an ihn.

§ 19 Datenschutz durch Gestaltung von Technik und datenschutzfreundliche Voreinstellungen

(1) Sowohl für die als auch bei der Verarbeitung personenbezogener Daten stellt der Verantwortliche durch Gestaltung seiner technischen Systeme sicher, dass die Grundsätze des § 3 umgesetzt

werden. Dies gilt insbesondere für die personenbezogenen Daten besonderer Kategorien und die Einschränkung der Verarbeitung personenbezogener Daten.

(2) Der Verantwortliche stellt durch Voreinstellungen sicher, dass nur solche personenbezogenen Daten verarbeitet werden können, die für den jeweiligen Zweck der Verarbeitung erforderlich sind. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, die Dauer ihrer Speicherung und den Zugang zu diesen Daten. Durch Voreinstellungen dürfen die personenbezogenen Daten nicht automatisiert ohne Eingreifen des Verantwortlichen einer unbestimmten Anzahl von Personen zugänglich gemacht werden.

§ 20 Sicherheit der Datenverarbeitung

(1) Der Verantwortliche stellt auf der Grundlage einer Bewertung der Risiken nach § 17 Absatz 2 sicher, dass

1. grundsätzlich nur personenbezogene Daten, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden,
2. nur Befugte personenbezogene Daten zur Kenntnis nehmen können,
3. personenbezogene Daten und die zu ihrer Verarbeitung vorgesehenen Systeme und Dienste zur Verfügung stehen,
4. personenbezogene Daten unversehrt, vollständig und aktuell bleiben und die zur Verarbeitung eingesetzten Prozesse und Systeme die festgelegten Anforderungen fortlaufend erfüllen,
5. die Verarbeitung transparent erfolgt, insbesondere
 - a) die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, die eine Nachvollziehbarkeit zeitnah ermöglicht,
 - b) personenbezogene Daten ihrem Ursprung zugeordnet werden können und



- c) festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat,
6. die Datenverarbeitung so organisiert und die eingesetzten technischen Systeme so gestaltet sind, dass eine Ausübung der Rechte der betroffenen Person ungehindert erfolgen kann,
7. die Verarbeitung personenbezogener Daten ausschließlich im Rahmen von zuvor bestimmten Befugnissen für vorab festgelegte rechtmäßige Zwecke erfolgt und die Daten hierfür nach den jeweiligen Zwecken und nach den jeweils betroffenen Personen getrennt werden können.

(2) Die Bediensteten dürfen sich von personenbezogenen Daten nur Kenntnis verschaffen, soweit dies zur Erfüllung der ihnen obliegenden Aufgaben oder für die zur gemeinsamen Aufgabenerfüllung notwendige Zusammenarbeit erforderlich ist. Sind personenbezogene Daten derart verbunden, dass ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch Kenntnisnahme und Offenlegung derjenigen Daten, die nicht zur Erreichung des jeweiligen Zweckes nach § 1 Absatz 1 erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der betroffenen Person oder Dritter überwiegen. Diese Daten dürfen nicht weiterverarbeitet werden.

(3) Im Justiz- und Maßregelvollzug sind Gesundheits- und Therapieakten, psychologische und pädagogische Testunterlagen und Krankenblätter getrennt von anderen Unterlagen zu führen und durch technische und organisatorische Maßnahmen gegen unbefugten Zugang und unbefugten Gebrauch besonders zu sichern.

§ 21 Datenschutz-Folgenabschätzung

(1) Der Verantwortliche nimmt eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten vor, wenn deren Form, insbesondere bei Verwendung neuer Technologien aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hat.

(2) Für ähnliche Verarbeitungsvorgänge mit vergleichbar hohem Risikopotenzial kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche beteiligt die oder den behördlichen Datenschutzbeauftragten an der Durchführung der Datenschutz-Folgenabschätzung.

(4) Die Datenschutz-Folgenabschätzung hat den Rechten und den schutzwürdigen Interessen der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. die Zwecke der Verarbeitung,
2. eine Beschreibung der geplanten Verarbeitungsvorgänge nach Kategorien,
3. eine Bewertung der Erforderlichkeit und Angemessenheit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
4. eine Bewertung der Risiken für die Rechtsgüter der betroffenen Personen und deren schutzwürdige Interessen sowie
5. die technischen und organisatorischen Maßnahmen zur Abwendung und Verringerung der Risiken.

§ 22 Zusammenarbeit mit der oder dem Landesbeauftragten

Der Verantwortliche, der Auftragsverarbeiter und die oder der Landesbeauftragte arbeiten bei der Erfüllung der ihnen durch oder aufgrund dieses Gesetzes übertragenen Aufgaben eng und frühzeitig zusammen.

§ 23 Anhörung der oder des Landesbeauftragten

(1) Der Verantwortliche hört vor der Inbetriebnahme neuer Dateisysteme die Landesbeauftragte oder den Landesbeauftragten an, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 21 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hätte, soweit der Verantwortliche keine Maßnahmen zur Abwendung oder Verringerung des Risikos trifft oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien oder Verfahren, ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Landesbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die den Verantwortlichen zu einer Anhörung nach Satz 1 verpflichten.

(2) Der Verantwortliche übermittelt der oder dem Landesbeauftragten neben der Datenschutz-Folgenabschätzung und dem Namen und der Erreichbarkeit der oder des behördlichen Datenschutzbeauftragten Angaben zu den jeweiligen Zuständigkeiten des oder der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter. Auf Anforderung übermittelt der Verantwortliche unverzüglich weitere Angaben, die die oder der Landesbeauftragte benötigt, um die Rechtmäßigkeit der Verarbeitung sowie die Risiken und die Maßnahmen zu deren Abwendung oder Verringerung bewerten zu können.

(3) Kommt die oder der Landesbeauftragte zu dem Ergebnis, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche die Risiken nicht ausreichend ermittelt oder ausreichende Maßnahmen zu deren Abwendung oder Verringerung noch nicht getroffen hat, übermittelt sie oder er dem Verantwortlichen und erforderlichenfalls dem Auftragsverarbeiter schriftlich innerhalb von sechs Wochen nach Einleitung der Anhörung Empfehlungen zu den noch zu ergreifenden Maßnahmen. Die oder der Landesbeauftragte kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders umfangreich oder schwierig ist. Sie oder er unterrichtet in diesem Fall den Verantwortlichen und erforderlichenfalls den Auftragsverarbeiter innerhalb eines Monats nach Einleitung der Anhörung unter Mitteilung der Gründe über die Fristverlängerung. Die Befugnisse der oder des Landesbeauftragten nach § 36 bleiben unberührt.

(4) Ist die beabsichtigte Verarbeitung aufgrund ihrer erheblichen Bedeutung für die Aufgabenerfüllung besonders dringlich, kann der Verantwortliche 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 nachträglich zu berücksichtigen und die Art und Weise der Verarbeitung erforderlichenfalls entsprechend anzupassen.

§ 24 Verzeichnis der Verarbeitungstätigkeiten

(1) Der Verantwortliche führt schriftlich oder elektronisch ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Es enthält folgende Angaben:

1. den Namen und die Erreichbarkeit des oder der gemeinsam Verantwortlichen sowie der oder des behördlichen Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. die Rechtsgrundlagen der Verarbeitung,
4. die Kategorien
 - a) betroffener Personen,
 - b) personenbezogener Daten,
 - c) von Empfängern und
 - d) der Übermittlung personenbezogener Daten an einen Drittstaat oder an eine internationale Organisation,
5. die gesetzlich vorgesehenen Regel- und Höchstfristen für die Löschung verschiedener Kategorien personenbezogener Daten, hilfsweise die vorgesehenen Fristen zur Überprüfung der weiteren Erforderlichkeit der Speicherung personenbezogener Daten,
6. die Verwendung von Profiling,



7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 17.

(2) Der Auftragsverarbeiter führt schriftlich oder elektronisch ein Verzeichnis über alle Kategorien von Verarbeitungstätigkeiten, die er im Auftrag eines Verantwortlichen durchführt. Es enthält folgende Angaben:

1. den Namen und die Erreichbarkeit des Auftragsverarbeiters, der von ihm hinzugezogenen Auftragsverarbeiter sowie der Verantwortlichen, in deren Auftrag er tätig ist, und seiner oder seines Datenschutzbeauftragten,
2. die Kategorien von Verarbeitungstätigkeiten, die er im Auftrag des Verantwortlichen durchführt,
3. die von dem Verantwortlichen angewiesene Übermittlung personenbezogener Daten an einen Drittstaat oder eine internationale Organisation unter Angabe des Staates oder der Organisation und
4. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 17.

(3) Der Verantwortliche und der Auftragsverarbeiter stellen ihre Verzeichnisse der oder dem Landesbeauftragten auf Anforderung zur Verfügung.

§ 25 Protokollierung

(1) In automatisierten Verarbeitungssystemen sind zumindest die folgenden Verarbeitungsvorgänge zu protokollieren:

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

5. Kombination,

6. Löschung und

7. Einschränkung der Verarbeitung.

(2) Die Protokolle über Abfragen und Offenlegungen ermöglichen die Feststellung

1. des Datums und der Uhrzeit der Abfrage oder Offenlegung,

2. der die personenbezogenen Daten abfragenden oder offenlegenden Personen und des Grundes ihrer Abfrage oder Offenlegung und

3. der Empfänger personenbezogener Daten.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die behördlichen Datenschutzbeauftragten, die Landesbeauftragte oder den Landesbeauftragten und den Verantwortlichen sowie für die Gewährleistung des in § 3 Nummer 6 enthaltenen Grundsatzes der Integrität und Vertraulichkeit verwendet werden. Die Protokolldaten dürfen auch

1. im Zusammenhang mit einer Verletzung des Datengeheimnisses

a) zur Verfolgung von Straftaten und Ordnungswidrigkeiten oder

b) für arbeits-, beamten- oder disziplinarrechtliche Maßnahmen sowie

2. zur Verfolgung von Straftaten von erheblicher Bedeutung

verarbeitet werden.

(4) Die Protokolldaten sind zu löschen, wenn sie zu den in Absatz 3 Satz 1 genannten Zwecken nicht mehr erforderlich sind. Im Justiz- und Maßregelvollzug erfolgt die Löschung der Protokolldaten zwei Jahre nach ihrer Erstellung.



(5) Der Verantwortliche und der Auftragsverarbeiter stellen die Protokolle der oder dem Landesbeauftragten auf Anforderung zur Verfügung.

Abschnitt 4

An der Datenverarbeitung Beteiligte

§ 26 Datengeheimnis

(1) Die mit der Verarbeitung von Daten befassten Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Personen, die nicht Amtsträger nach § 11 Absatz 1 Nummer 2 des Strafgesetzbuches sind, sind vor der Aufnahme ihrer Tätigkeit über die zu beachtenden Bestimmungen zu unterrichten und auf deren Einhaltung förmlich gemäß § 1 des Verpflichtungsgesetzes zu verpflichten.

(2) Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

§ 27 Datenverarbeitung im Auftrag

(1) Beauftragt der Verantwortliche andere Personen oder Stellen mit der Verarbeitung personenbezogener Daten, bleibt er für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind ihm gegenüber geltend zu machen.

(2) Der Verantwortliche darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Rahmen der gesetzlichen Vorgaben erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines schriftlichen Vertrags oder eines anderen Rechtsinstruments, in dem der Gegenstand, die Dauer, der Zweck der Verarbeitung sowie die Kategorien der Verarbeitungstätigkeiten, der personenbezogenen Daten und der betroffenen Personen sowie die Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters festgelegt sind. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

1. dem Verantwortlichen unverzüglich mitteilt, wenn er eine Anweisung für rechtswidrig hält,
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Verschwiegenheit verpflichtet werden, soweit sie einer gesetzlichen Verschwiegenheitspflicht nicht unterliegen,
3. den Verantwortlichen bei der Einhaltung der Bestimmungen über die Rechte der betroffenen Person unterstützt,
4. alle personenbezogenen Daten nach Abschluss der zu erbringenden Leistungen entweder zurückgibt oder löscht und Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht,
5. dem Verantwortlichen alle erforderlichen Unterlagen, insbesondere die gemäß § 25 erstellten Protokolle, zum Nachweis der Einhaltung seiner gesetzlichen und vertraglichen Verpflichtungen zur Verfügung stellt,
6. Kontrollen, die von dem Verantwortlichen oder einem von diesem hiermit Beauftragten durchgeführt werden, ermöglicht und unterstützt,
7. die Bestimmungen dieses Gesetzes für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters beachtet,
8. alle gemäß den §§ 17, 19 und 20 erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Erkenntnisse den Verantwortlichen bei der

Einhaltung der in den §§ 20, 21, 23, 29 und 30 genannten Pflichten unterstützt.

(4) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unbefugt festlegt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

(5) Die Hinzuziehung weiterer Auftragsverarbeiter bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen. Hat der Verantwortliche eine allgemeine Zustimmung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, unterrichtet der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung. Der Verantwortliche kann die Hinzuziehung oder Ersetzung von weiteren Auftragsverarbeitern untersagen.

(6) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so erlegt er diesem die Verpflichtungen aus dem Vertrag oder dem anderen Rechtsinstrument nach Absatz 3 auf, die auch für ihn gelten, soweit diese für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Bestimmungen bestehen. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht und entsteht dem Verantwortlichen hieraus ein Schaden, so haftet der Auftragsverarbeiter hierfür und hat dessen Verschulden in gleichem Umfang zu vertreten wie eigenes.

§ 28 Gemeinsam Verantwortliche

(1) Soweit zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung personenbezogener Daten festlegen, sind sie gemeinsam verantwortlich.

(2) Sie legen ihre jeweiligen Aufgaben und datenschutzrechtlichen Pflichten in transparenter Form in einer Vereinbarung fest, wenn sich diese nicht bereits aus Rechtsvorschriften ergeben. Aus der Vereinbarung muss insbesondere hervorgehen, wer den Pflichten nach den §§ 5, 7 und 8 nachzukommen hat und wie und gegenüber wem die betroffene Person ihre Rechte nach den §§ 40 und 41 wahrnehmen kann. Der gemeinsam Verantwortliche, an den sich die betroffene Person wendet, leitet das Anliegen an den jeweils zuständigen gemeinsam Verantwortlichen weiter.

Abschnitt 5

Verletzung der Sicherheit personenbezogener Daten

§ 29 Meldung an die Landesbeauftragte oder den Landesbeauftragten

(1) Der Verantwortliche meldet eine Verletzung der Sicherheit personenbezogener Daten unverzüglich der oder dem Landesbeauftragten, es sei denn, es ist absehbar, dass die Verletzung nicht zu einer Beeinträchtigung der Rechtsgüter der betroffenen Person führt. Erfolgt die Meldung nicht binnen 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter meldet dem Verantwortlichen unverzüglich eine Verletzung der Sicherheit personenbezogener Daten. Absatz 1 Satz 2 gilt entsprechend.

(3) Die Meldung nach Absatz 1 enthält zumindest folgende Angaben:

1. die Art der Verletzung der Sicherheit personenbezogener Daten, einschließlich der Kategorien und der Anzahl sowohl der betroffenen Personen als auch der betroffenen personenbezogenen Datensätze,
2. den Namen und die Erreichbarkeit der oder des behördlichen Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Angaben machen kann,
3. die voraussichtlichen Folgen der Verletzung der Sicherheit personenbezogener Daten und
4. die von dem Verantwortlichen ergriffenen oder vorgesehenen Maßnahmen zur Behebung der Verletzung und zur Verringerung möglicher nachteiliger Auswirkungen.

Der Verantwortliche reicht die zum Zeitpunkt der Meldung noch nicht vorliegenden Erkenntnisse unverzüglich nach.



(4) Der Verantwortliche dokumentiert die Verletzung der Sicherheit personenbezogener Daten, einschließlich der Auswirkungen und Abhilfemaßnahmen, sowie die Gründe für eine Unterlassung der Meldung nach Absatz 1.

(5) Soweit in den Fällen des Absatzes 1 personenbezogene Daten betroffen sind, die von einem oder an einen anderen Verantwortlichen übermittelt wurden, sind diesem die in Absatz 3 genannten Angaben unverzüglich mitzuteilen.

§ 30 Unterrichtung der betroffenen Person

(1) Gefährdet eine Verletzung der Sicherheit personenbezogener Daten voraussichtlich die Rechtsgüter einer Person erheblich, so unterrichtet der Verantwortliche diese hierüber unverzüglich.

(2) Die Unterrichtung nach Absatz 1 enthält in klarer und einfacher Sprache die Art der Verletzung der Sicherheit personenbezogener Daten und zumindest die in § 29 Absatz 3 Satz 1 Nummer 2 bis 4 genannten Angaben. Ist die Unterrichtung der betroffenen Person mit einem unverhältnismäßigen Aufwand verbunden, stellt der Verantwortliche deren Unterrichtung durch eine öffentliche Bekanntgabe oder eine vergleichbare Maßnahme sicher.

(3) Von der Unterrichtung nach Absatz 1 kann abgesehen werden, wenn

1. bereits zuvor von dem Verantwortlichen für eine solche Verletzung der Sicherheit getroffene technische und organisatorische Maßnahmen, namentlich Verschlüsselungen, die betreffenden personenbezogenen Daten umfassen und diese so für unbefugte Personen unzugänglich gemacht wurden oder
2. der Verantwortliche die erhebliche Gefährdung nach Absatz 1 durch unmittelbar nach der Verletzung getroffene Maßnahmen voraussichtlich abgewendet hat.

(4) Die Unterrichtung nach Absatz 1 kann unter den Voraussetzungen des § 8 Absatz 2 aufgeschoben, eingeschränkt oder unterlassen werden.

(5) Hat der Verantwortliche die betroffene Person über eine Verletzung der Sicherheit personenbezogener Daten nicht unterrichtet, kann die oder der Landesbeauftragte unter Berücksichtigung der Wahrscheinlichkeit, mit der der Verstoß zu einer erheblichen Gefährdung der Rechtsgüter der betroffenen Person führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder förmlich feststellen, dass nach ihrer oder seiner Auffassung die in Absatz 3 oder Absatz 4 genannten Voraussetzungen erfüllt sind.

Abschnitt 6

Behördliche Datenschutzbeauftragte

§ 31 Bestellung

(1) Der Verantwortliche bestellt eine Bedienstete oder einen Bediensteten aufgrund ihrer oder seiner beruflichen Qualifikation, insbesondere ihres oder seines datenschutzrechtlichen Fachwissens sowie ihrer oder seiner Eignung zur Erfüllung der Aufgaben nach § 33 zur oder zum behördlichen Datenschutzbeauftragten.

(2) Die Bestellung kann unter Berücksichtigung von Organisationsstruktur und Größe für mehrere öffentliche Stellen gemeinsam erfolgen.

(3) Der Verantwortliche teilt der oder dem Landesbeauftragten den Namen und die Erreichbarkeit der oder des behördlichen Datenschutzbeauftragten mit.

§ 32 Stellung und Rechte

(1) Der Verantwortliche stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Personenbezogene Daten einer betroffenen Person, der von dem Verantwortlichen, soweit gesetzlich vorgesehen, Vertraulichkeit oder Geheimhaltung besonders zugesichert worden ist,

dürfen der oder dem behördlichen Datenschutzbeauftragten nicht offenbart werden.

(2) Der Verantwortliche unterstützt die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben nach § 33, indem er die hierfür sowie zur Erhaltung ihres oder seines Fachwissens erforderlichen Mittel zur Verfügung stellt und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen ermöglicht. Insbesondere ist die oder der behördliche Datenschutzbeauftragte von der Erledigung anderer Aufgaben freizustellen.

(3) Der Verantwortliche stellt sicher, dass die oder der behördliche Datenschutzbeauftragte fachlichen Weisungen nicht unterliegt.

(4) Die oder der behördliche Datenschutzbeauftragte darf wegen der Erfüllung ihrer oder seiner Aufgaben nicht benachteiligt werden. Sie oder er ist vor Kündigung in gleicher Weise geschützt wie ein Mitglied des Personalrats.

(5) Die betroffene Person kann sich mit Fragen zur Verarbeitung ihrer personenbezogenen Daten und zur Wahrnehmung ihrer Rechte an die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten wenden. Die oder der behördliche Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf diese zulassen, verpflichtet, soweit sie oder er hiervon nicht durch die betroffene Person entbunden wird. Dies gilt auch nach Beendigung der Tätigkeit als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter.

§ 33 Aufgaben

Die oder der behördliche Datenschutzbeauftragte hat insbesondere folgende Aufgaben:

1. Unterrichtung und Beratung des Verantwortlichen und seiner Bediensteten hinsichtlich ihrer Pflichten nach diesem Gesetz, insbesondere zu der Datenschutz-Folgenabschätzung, und nach sonstigen Vorschriften über den Datenschutz,

2. Überwachung der Einhaltung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften sowie der Maßnahmen des Verantwortlichen zum Schutz personenbezogener Daten,
3. Zusammenarbeit mit der oder dem Landesbeauftragten sowie Ausübung der Funktion als deren oder dessen Ansprechpartner.

Abschnitt 7

Datenschutzrechtliche Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten

§ 34 Aufgaben

- (1) Die oder der Landesbeauftragte hat die Aufgaben,
 1. die Einhaltung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu überwachen,
 2. die Öffentlichkeit auf die mit der Verarbeitung personenbezogener Daten zusammenhängenden Risiken hinzuweisen und sie über die gesetzlichen Bestimmungen, insbesondere die Rechtsgrundlagen, Verfahrensgarantien und die Rechte der betroffenen Personen aufzuklären,
 3. den Landtag, die Landesregierung und die in § 1 genannten Stellen bei Gesetzgebungsvorhaben und Verwaltungsmaßnahmen zum Schutz der Rechtsgüter betroffener Personen in Bezug auf die Verarbeitung personenbezogener Daten, insbesondere durch die Abgabe von Stellungnahmen, zu beraten,
 4. Verantwortliche und Auftragsverarbeiter auf die ihnen aus den Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/680 entstehenden Pflichten hinzuweisen,
 5. der betroffenen Person auf Antrag Hinweise für die Ausübung ihrer Rechte nach den zur Umsetzung der Richtlinie (EU) 2016/680

erlassenen Rechtsvorschriften zu erteilen und erforderlichenfalls dazu mit den Landesbeauftragten anderer Länder, der oder dem Bundesbeauftragten oder den Datenschutzbeauftragten anderer Mitgliedstaaten der Europäischen Union zusammenzuarbeiten,

6. Beschwerden gemäß § 42 nachzugehen und die betroffene Person innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Überprüfung zu unterrichten,
7. in den Fällen der §§ 40 und 41, in denen die Rechte der betroffenen Person durch sie oder ihn ausgeübt werden, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung zu unterrichten oder ihr die Gründe mitzuteilen, aus denen von einer Überprüfung abgesehen wurde,
8. mit anderen Landesbeauftragten, der oder dem Bundesbeauftragten und den Datenschutzbeauftragten anderer Mitgliedstaaten der Europäischen Union zusammenzuarbeiten und ihnen Amtshilfe zu leisten, um die Einhaltung und eine einheitliche Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu gewährleisten,
9. die Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, auch auf der Grundlage von Erkenntnissen anderer Landesbeauftragter, der oder des Bundesbeauftragten oder der Datenschutzbeauftragten anderer Mitgliedstaaten der Europäischen Union oder einer anderen öffentlichen Stelle, zu untersuchen,
10. maßgebliche Entwicklungen, insbesondere der Informations- und Kommunikationstechnologie, soweit sie sich auf den Schutz personenbezogener Daten auswirken, zu beobachten und
11. den Verantwortlichen vor Inbetriebnahme neuer Datenverarbeitungssysteme nach § 23 zu beraten.

(2) Die oder der Landesbeauftragte erleichtert betroffenen Personen die Einlegung von Beschwerden durch Maßnahmen wie die Bereitstellung eines Formulars.

(3) Die Inanspruchnahme der oder des Landesbeauftragten ist grundsätzlich unentgeltlich. Bei offenkundig unbegründeten oder, insbesondere im Fall häufiger Wiederholung, exzessiven Anträgen der betroffenen Person kann die oder der Landesbeauftragte eine angemessene Gebühr verlangen oder sich weigern, aufgrund der Eingabe tätig zu werden. In diesem Fall dokumentiert sie oder er die Gründe für den offenkundig unbegründeten oder exzessiven Charakter.

§ 35 Unterstützung durch Verantwortliche und Auftragsverarbeiter

(1) Verantwortliche und Auftragsverarbeiter sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen.

(2) Ihr oder ihm ist insbesondere

1. Auskunft zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen und
2. Zutritt zu allen Diensträumen, in denen personenbezogene Daten verarbeitet werden, einschließlich aller Datenverarbeitungsanlagen und Geräte, zu gewähren,

soweit dies zur Erfüllung ihrer oder seiner Aufgaben erforderlich ist. Der Verantwortliche kann nach Satz 1 Nummer 1 auch eine elektronische Einsichtnahme gewähren.

(3) Absatz 2 Nummer 1 gilt nicht, soweit

1. das jeweils zuständige Mitglied der Landesregierung im Einzelfall feststellt, dass die Einsicht in die Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet oder
2. die Erteilung einer Auskunft oder die Einsichtnahme personenbezogener Daten einer Person betreffen, der von dem Verant-

wortlichen, soweit gesetzlich vorgesehen, Vertraulichkeit oder Geheimhaltung besonders zugesichert worden ist.

(4) Berufs- und Amtsgeheimnisse entbinden nicht von der Unterstützungspflicht nach Absatz 1.

§ 36 Befugnisse

(1) Die oder der Landesbeauftragte kann zur Erfüllung ihrer oder seiner Aufgaben

1. Verantwortliche oder Auftragsverarbeiter warnen, dass die beabsichtigte Verarbeitung personenbezogener Daten voraussichtlich gegen die zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften verstößt oder
2. gegenüber Verantwortlichen oder Auftragsverarbeitern Verstöße gegen die zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten beanstanden.

Die oder der Landesbeauftragte teilt die Warnung oder Beanstandung dem jeweils zuständigen Mitglied der Landesregierung und erforderlichenfalls der betroffenen Person mit. Der Adressat der Warnung oder Beanstandung gibt innerhalb einer von der oder dem Landesbeauftragten zu bestimmenden Frist eine Stellungnahme ab, die auch die Maßnahmen enthalten soll, die aufgrund der Warnung oder Beanstandung getroffen worden sind.

(2) Die oder der Landesbeauftragte kann von einer Warnung oder Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt oder wenn deren Behebung sichergestellt ist.

(3) Mit der Warnung oder Beanstandung soll die oder der Landesbeauftragte Vorschläge zur Beseitigung der Mängel und zur Verbesserung des Datenschutzes verbinden.

(4) Hat der Verantwortliche aufgrund der Warnung oder Beanstandung ausreichende Maßnahmen nicht ergriffen, kann die oder

der Landesbeauftragte zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Bestimmungen den Verantwortlichen oder Auftragsverarbeiter anweisen,

1. dem Antrag einer betroffenen Person auf Ausübung der ihr nach diesem Gesetz zustehenden Rechte zu entsprechen,
2. Verarbeitungsvorgänge auf bestimmte Weise und innerhalb einer bestimmten Frist in Einklang mit den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu bringen, insbesondere personenbezogene Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken und die Empfänger dieser Daten entsprechend zu unterrichten,
3. die von einer Verletzung der Sicherheit personenbezogener Daten betroffene Person entsprechend zu unterrichten.

(5) In den Fällen des § 34 Absatz 1 Nummer 7 darf die Unterrichtung der betroffenen Person keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht zugestimmt hat.

§ 37 Tätigkeitsbericht

(1) Die oder der Landesbeauftragte übermittelt dem Landtag und der Landesregierung jährlich einen Bericht über ihre oder seine Tätigkeiten nach diesem Gesetz. Die Landesregierung nimmt innerhalb von sechs Monaten gegenüber dem Landtag dazu Stellung.

(2) Der Bericht wird der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht.

§ 38 Zusammenarbeit zur einheitlichen Umsetzung der Richtlinie (EU) 2016/680

§ 82 des Bundesdatenschutzgesetzes gilt für die Übermittlung von Informationen der oder des Landesbeauftragten an die anderen Landesbeauftragten, die oder den Bundesbeauftragten und die Datenschutzbeauftragten anderer Mitgliedstaaten der Europäischen Union, auch im Wege der Amtshilfe, entsprechend.

Abschnitt 8

Rechte der betroffenen Person

§ 39 Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche verwendet gegenüber der betroffenen Person eine klare und einfache Sprache. Er wählt dabei eine leicht zugängliche, genaue und verständliche Form. Unbeschadet besonderer Formvorschriften soll er Eingaben grundsätzlich in der für sie gewählten Form beantworten.

(2) Der Verantwortliche unterrichtet die betroffene Person unverzüglich in Textform darüber, wie mit ihrer Eingabe verfahren wurde.

(3) Hat der Verantwortliche begründete Zweifel an der Identität der betroffenen Person, kann er die erforderlichen Auskünfte anfordern, um diese festzustellen.

(4) Die Tätigkeit des Verantwortlichen nach diesem Gesetz ist für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder, insbesondere im Fall häufiger Wiederholung, exzessiven Eingaben der betroffenen Person kann der Verantwortliche sich weigern, tätig zu werden. In diesem Fall trägt er die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Eingabe.

(5) Lehnt der Verantwortliche einen Antrag nach § 40 oder § 41 ab, so weist er die betroffene Person darauf hin, dass sie ihr Recht über die Landesbeauftragte oder den Landesbeauftragten ausüben oder bei ihr oder ihm Beschwerde einlegen kann.

(6) Der Verantwortliche dokumentiert die Gründe seiner Entscheidung.

§ 40 Recht auf Auskunft

(1) Der Verantwortliche erteilt der betroffenen Person auf Antrag Auskunft darüber, ob er deren personenbezogene Daten verarbei-

tet. Der Anspruch auf Auskunft umfasst darüber hinaus die Unterrichtung über

1. die gespeicherten personenbezogenen Daten und deren Kategorien,
2. Informationen zur Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, denen die Daten offengelegt worden sind,
5. die für die Daten geltende Dauer der Speicherung, hilfsweise die Kriterien für die Festlegung dieser Dauer,
6. das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten,
7. das Recht, die Landesbeauftragte oder den Landesbeauftragten anzurufen, sowie Angaben zu deren oder dessen Erreichbarkeit.

(2) Absatz 1 gilt nicht für Protokolldaten nach § 25.

(3) Von der Erteilung einer Auskunft ist abzusehen, wenn die betroffene Person Angaben, die das Auffinden der Daten ermöglichen, nicht macht und deshalb der hierfür erforderliche Aufwand außer Verhältnis zu den schutzwürdigen Interessen der betroffenen Person steht.

(4) Der Verantwortliche darf unter den Voraussetzungen des § 8 Absatz 2 von einer Auskunft absehen, diese aufschieben oder einschränken.

(5) Der Verantwortliche unterrichtet die betroffene Person unverzüglich schriftlich unter Angabe der Gründe über das Absehen von sowie das Aufschieben oder die Einschränkung der Erteilung einer Auskunft. Dies gilt nicht, wenn bereits diese Unterrichtung oder ihre Begründung den mit Absatz 4 verfolgten Zweck gefährden würde.

(6) Wird die betroffene Person nach Absatz 5 über das Absehen von, das Aufschieben oder die Einschränkung der Erteilung einer Aus-



kunft unterrichtet, kann sie ihr Recht auf Auskunft auch über die Landesbeauftragte oder den Landesbeauftragten ausüben. Macht die betroffene Person von diesem Recht Gebrauch, ist die Auskunft der oder dem Landesbeauftragten zu erteilen; § 35 Absatz 3 gilt entsprechend. Die oder der Landesbeauftragte unterrichtet die betroffene Person darüber, dass sie oder er, soweit gesetzlich zulässig, deren Recht auf Auskunft für sie ausgeübt hat, und über das Recht auf gerichtlichen Rechtsschutz.

(7) Die Auskunft kann auch durch die Gewährung von Akteneinsicht oder die Aushändigung von Ablichtungen oder Ausdrucken erteilt werden.

§ 41 Recht auf Berichtigung und Löschung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung der sie betreffenden unrichtigen Daten zu verlangen. Sie kann die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung des Zwecks der Verarbeitung angemessen ist.

(2) Kann die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden und ist deshalb anstelle der Berichtigung eine Einschränkung der Verarbeitung erfolgt, unterrichtet der Verantwortliche die betroffene Person, bevor er die Einschränkung wieder aufhebt.

(3) Die betroffene Person kann unter den Voraussetzungen des § 15 die Löschung der sie betreffenden personenbezogenen Daten verlangen.

(4) Der Verantwortliche unterrichtet die betroffene Person schriftlich über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung unter Angabe der Gründe.

(5) Die Unterrichtung oder ihre Begründung nach Absatz 4 kann unter den Voraussetzungen des § 8 Absatz 2 ganz oder teilweise eingeschränkt werden oder unterbleiben. In diesem Fall kann die betroffene Person ihr Recht auf Unterrichtung nach Absatz 4 über die

Landesbeauftragte oder den Landesbeauftragten ausüben. Macht sie von diesem Recht Gebrauch, unterrichtet der Verantwortliche die Landesbeauftragte oder den Landesbeauftragten über die Gründe für das Absehen von der Berichtigung oder Löschung oder die an deren Stelle tretende Einschränkung der Verarbeitung; § 35 Absatz 3 gilt entsprechend. Die oder der Landesbeauftragte unterrichtet die betroffene Person darüber, dass sie oder er, soweit gesetzlich zulässig, deren Recht auf Unterrichtung für sie ausgeübt hat, und über das Recht auf gerichtlichen Rechtsschutz.

§ 42 Recht auf Beschwerde

(1) Die betroffene Person hat unbeschadet anderer Rechtsbehelfe das Recht, sich mit einer Beschwerde an die Landesbeauftragte oder den Landesbeauftragten zu wenden, wenn sie der Auffassung ist, von einem Verantwortlichen oder einem Auftragsverarbeiter durch die Verarbeitung ihrer personenbezogenen Daten zu den in § 1 Absatz 1 genannten Zwecken in ihren Rechten verletzt worden zu sein.

(2) Die oder der Landesbeauftragte unterrichtet die betroffene Person über den Stand und das Ergebnis ihrer oder seiner Prüfung und weist sie auf die Möglichkeit gerichtlichen Rechtsschutzes hin.

(3) Die oder der Landesbeauftragte leitet eine bei ihr oder ihm erhobene Beschwerde, die in die Zuständigkeit einer oder eines anderen Landesbeauftragten oder der oder des Bundesbeauftragten fällt, unverzüglich an diese oder diesen weiter. Sie oder er unterrichtet die betroffene Person über die Weiterleitung und leistet ihr auf deren Ersuchen weitere Unterstützung.

§ 43 Schadensersatz

(1) Hat ein Verantwortlicher einer Person durch eine Verarbeitung personenbezogener Daten, die nach den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften rechtswidrig war, einen Schaden zugefügt, ist er der Person zum Schadensersatz verpflichtet, es sei denn, ihn trifft kein Verschulden.

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



(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welcher von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haften sie als Gesamtschuldner.

(4) Ein Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen Pflichten nach § 27 Absatz 3 nicht nachgekommen ist oder gegen rechtmäßig erteilte Anweisungen des Verantwortlichen verstoßen hat, es sei denn, ihn trifft kein Verschulden.

(5) Bei einem Mitverschulden der betroffenen Person oder eines Dritten ist § 254 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuches entsprechende Anwendung.

Abschnitt 9

Gerichtlicher Rechtsschutz und Schlussvorschriften

§ 44 Gerichtlicher Rechtsschutz

Für Streitigkeiten zwischen einem Verantwortlichen, einem Auftragsverarbeiter oder einer betroffenen Person und der oder dem Landesbeauftragten über Rechte und Pflichten nach den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften gilt § 20 des Bundesdatenschutzgesetzes entsprechend.

§ 45 Einschränkung eines Grundrechts

Durch dieses Gesetz wird das Grundrecht auf Datenschutz (Artikel 11 Absatz 1 der Verfassung des Landes Brandenburg) eingeschränkt.

§ 46 Übergangsregelung

Bis zum 6. Mai 2023 ist § 25 für automatisierte Dateisysteme, die vor dem 6. Mai 2016 eingerichtet worden sind, nicht anzuwenden.



Kontakt

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon 033203 356-0

Fax 033203 356-49

E-Mail Poststelle@LDA.Brandenburg.de

WWW.LDA.BRANDENBURG.DE