Gesetz zum Schutz personenbezogener Daten
(Datenschutzgesetz Nordrhein-Westfalen – DSG NRW –)

in der Fassung der Bekanntmachung vom 9. Juni 2000 zuletzt geändert durch Gesetz vom 29. April 2003 (GV. NRW. 2003, S. 252)

Inhaltsverzeichnis

Erster Teil - Allgemeiner Datenschutz

Erster Abschnitt - Allgemeine Bestimmungen

§ 1 Aufgabe
§ 2 Anwendungsbereich
§ 3 Begriffsbestimmungen
§ 4 Zulässigkeit der Datenverarbeitung
§ 4a Verbunddateien
§ 5 Rechte der betroffenen Person
§ 6 Datengeheimnis
§ 7 Sicherstellung des Datenschutzes
§ 8 Verfahrensverzeichnis
§ 9 Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung
§ 10 Technische und organisatorische Maßnahmen
§ 10a Datenschutzaudit
§ 11 Verarbeitung personenbezogener Daten im Auftrag

Zweiter Abschnitt - Rechtsgrundlagen der Datenverarbeitung

§ 12 Erhebung
§ 13 Zweckbindung bei Speicherung, Veränderung und Nutzung
§ 14 Übermittlung innerhalb des öffentlichen Bereichs
§ 15 Übermittlung an öffentlich-rechtliche Religionsgesellschaften
§ 16 Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs
§ 17 Übermittlung an ausländische Stellen

Dritter Abschnitt - Rechte der betroffenen Person

§ 18 Auskunft, Einsichtnahme
§ 19 Berichtigung, Sperrung und Löschung
§ 20 Schadensersatz

Zweiter Teil - Landesbeauftragter für Datenschutz und Informationsfreiheit

§ 21 Berufung und Rechtsstellung
§ 22 Aufgaben und Befugnisse § 23 (aufgehoben)
§ 24 Beanstandungen durch den Landesbeauftragten
§ 25 Anrufungsrecht der betroffenen Person
§ 26 (aufgehoben)
§ 27 Datenschutzbericht

Dritter Teil - Besonderer Datenschutz

§ 28 Datenverarbeitung für wissenschaftliche Zwecke
§ 29 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
§ 29a Mobile personenbezogene Datenverarbeitungssysteme
§ 29b Optisch-elektronische Überwachung
§ 30 Fernmessen und Fernwirken
§ 31 Nutzung von Verwaltungsdaten für die Erstellung von Statistiken
§ 32 Nutzung von Einzelangaben aus der amtlichen Statistik durch Gemeinden und Gemeindeverbände
§ 32a Behördliche Datenschutzbeauftragte

Vierter Teil - Straf- und Bußgeldvorschriften; Übergangsvorschriften

§ 33 Straftaten
§ 34 Ordnungswidrigkeiten
§ 35 Übergangsvorschriften
§ 36 Berichtspflicht

Erster Teil
Allgemeiner Datenschutz

Erster Abschnitt Allgemeine Bestimmungen

§ 1

Aufgabe

Aufgabe dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise

in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

§ 2 Anwendungsbereich

(1) Dieses Gesetz gilt für 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 (öffentliche Stellen), soweit diese personenbezogene Daten verarbeiten. Für den Landtag und für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz, soweit sie Verwaltungsaufgaben wahrnehmen; darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen, nur die Vorschriften des Zweiten Teils dieses Gesetzes. Für den Landesrechnungshof und die Staatlichen Rechnungsprüfungsämter gelten der Dritte Abschnitt des Ersten Teils und der Zweite Teil sowie die §§ 8 und 32 a nur, soweit sie Verwaltungsaufgaben wahrnehmen. Für die Ausübung des Gnadenrechts findet das Gesetz keine Anwendung.

(2) Von den Vorschriften dieses Gesetzes gelten nur die Vorschriften des Zweiten Teils sowie die §§ 8, 28 bis 31 und 32a dieses Gesetzes, soweit

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

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Im Übrigen sind mit Ausnahme der §§ 4 d bis 4 g sowie des § 38 die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anzuwenden. Unbeschadet der Regelung des Absatzes 1 Satz 1 gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes.

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

§ 3

Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person).

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Einzelnen ist

1. Erheben (Erhebung) das Beschaffen von Daten über die betroffene Person,
2. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,
4. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft,
5. Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten,
6. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,
7. Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten,

ungeachtet der dabei angewendeten Verfahren.

(3) Verantwortliche Stelle ist die Stelle im Sinne des § 2 Abs. 1, die personenbezogene Daten in eigener Verantwortung selbst verarbeitet oder in ihrem Auftrag von einer anderen Stelle verarbeiten lässt.

(4) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle a ußerhalb der verantwortlichen Stelle. Dritte sind nicht die betroffene Person sowie diejenigen Personen oder Stellen, die im Inland oder im übrigen Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag verarbeiten.

(5) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft.

(6) Eine Akte ist jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(8) Pseudonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der

Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die Daten verarbeitende Stelle darf keinen Zugriff auf die Zuordnungsfunktion haben; diese ist an dritter Stelle zu verwahren.

§ 4

Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

a) dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
b) die betroffene Person eingewilligt hat.

Die Einwilligung ist die widerrufliche, freiwillige und eindeutige Willenserklärung der betroffenen Person, einer bestimmten Datenverarbeitung zuzustimmen. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die betroffene Person auf die Einwilligung schriftlich besonders hinzuweisen. Sie ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger der Daten aufzuklären; sie ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann. Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

1. sie nur durch eine eindeutige und bewusste Handlung der handelnden Person erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber erkannt werden kann,
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird und
5. der betroffenen Person jederzeit Auskunft über den Inhalt ihrer Einwilligung gegeben werden kann.

(2) Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiterzuverarbeiten (Datenvermeidung). Produkte und Verfahren, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren (Datenschutzaudit) festgestellt wurde, sollen vorrangig berücksichtigt werden.

(3) Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben ist nur zulässig, wenn sie in einer Rechtsvorschrift geregelt ist, die den Zweck der Verarbeitung bestimmt sowie angemessene Garantien zum Schutz des Rechtes auf informationelle Selbstbestimmung vorsieht. Darüber hinaus ist die Verarbeitung dieser Daten zulässig, wenn

1. die betroffene Person eingewilligt hat,
2. sie ausschließlich im Interesse der betroffenen Person liegt,
3. sie sich auf Daten bezieht, die die betroffene Person selbst öffentlich gemacht hat,
4. sie
    a. auf der Grundlage der §§ 15, 28 und 29,
    b. zur Geltendmachung rechtlicher Ansprüche vor Gericht oder
    c. für die Abwehr von Gefahren für die öffentliche Sicherheit, für Zwecke der Strafrechtspflege oder zum Schutz vergleichbarer Rechtsgüter erforderlich ist.

(4) Soweit gesetzlich unter Wahrung der berechtigten Interessen der betroffenen Person nichts anderes bestimmt ist, dürfen Entscheidungen, die für die betroffene Person eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten zum Zweck der Bewertung einzelner Persönlichkeitsmerkmale gestützt werden, ohne dass der betroffenen Person die Geltendmachung der eigenen Interessen möglich gemacht worden ist.
(5) Wenn die betroffene Person schriftlich begründet, dass der im Übrigen rechtmäßigen Verarbeitung ihrer Daten oder einer bestimmten Datenverarbeitungsform ein schutzwürdiges besonderes persönliches Interesse entgegensteht, erfolgt die Verarbeitung ihrer personenbezogenen Daten nur, wenn eine Abwägung im Einzelfall ergibt, dass das Interesse der datenverarbeitenden Stelle gegenüber dem Interesse der betroffenen Person überwiegt. Die betroffene Person ist über das Ergebnis zu unterrichten.
(6) 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 in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, sind auc h 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 a
Verbunddateien

(1) Die Einrichtung gemeinsamer oder verbundener automatisierter Verfahren, in und aus denen mehrere öffentliche Stellen personenbezogene Daten verarbeiten sollen, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt. Die beteiligten Stellen haben die Datenart, die Aufgaben jeder beteiligten Stelle, den Zweck und den Umfang ihrer Verarbeitungsbefugnis sowie diejenige Stelle festzulegen, welche

die datenschutzrechtliche Verantwortung gegenüber den betroffenen Persone n trägt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist vorab zu unterrichten.
(2) Innerhalb einer öffentlichen Stelle bedarf die Einrichtung gemeinsamer oder verbundener automatisierter Verfahren, mit denen personenbezogene Daten aus unterschiedlichen Aufgabengebieten verarbeitet werden sollen, der Zulassung durch die Leitung der Stelle. Für die Zulässigkeit gilt Absatz 1 Satz 1 und 2 entsprechend.

§ 5

Rechte der betroffenen Person

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft, Einsichtnahme (§ 18),
2. Widerspruch aus besonderem Grund (§ 4 Abs. 5),
3. Unterrichtung (§§ 12 Abs. 2, 13 Abs. 2 Satz 2, 16 Abs. 1 Satz 2 und 3),
4. Berichtigung, Sperrung oder Löschung (§ 19),
5. Schadensersatz (§ 20),
6. Anrufung des Landesbeauftragten für Datenschutz und Informationsfreiheit (§ 25 Abs. 1),
7. Auskunft aus dem beim zuständigen behördlichen Datenschutzbeauftragten geführten Verfahrensverzeichnis (§ 8).

Diese Rechte können auch durch die Einwilligung der betroffenen Person nicht ausgeschlossen oder beschränkt werden.

§ 6

Datengeheimnis

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

§ 7

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 dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

§ 8

Verfahrensverzeichnis

(1) Jede datenverarbeitende Stelle, die für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten verantwortlich ist, hat in einem für den behördliche n Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens, einschließlich der eingesetzten Hard- und Software,
9. Fristen für die Sperrung und Löschung nach § 19 Abs. 2 und Abs. 3, 10.
10. eine beabsichtigte Datenübermittlung an Drittstaaten nach § 17 Abs. 2 und
11. Abs. 3, 11.die begründeten Ergebnisse der Vorabkontrollen nach § 10 Abs. 3 Satz 1.

(2) Die Angaben des Verfahrensverzeichnisses können bei der datenverarbeitenden Stelle von jeder Person eingesehen werden; dies gilt für die Angaben zu den Nummern 7, 8 und 11 nur, soweit dadurch die Sicherheit des technischen Verfahrens nicht beeinträchtigt wird. Satz 1 gilt nicht für

1. Verfahren nach dem Verfassungsschutzgesetz Nordrhein-Westfalen,
2. Verfahren, die der Gefahrenabwehr oder der Strafrechtspflege dienen,
3. Verfahren der Steuerfahndung,

soweit die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt. Die Gründe dafür sind aktenkundig zu machen und die antragstellende Person ist darauf hinzuweisen, dass sie sich an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden kann. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist auf sein Verlangen Einsicht zu gewähren.

§ 9

Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist.

(2) Die Ministerien 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 Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt. Die Datenempfänger, die Datenart und der Zweck des Abrufs sind festzulegen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist zu unterrichten.

(3) Die am Abrufverfahren beteiligten Stellen haben die nach § 10 erforderlichen Maßnahmen zu treffen.

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

(5) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden; dies gilt nicht für die betroffene Person.

(6) Die Absätze 1 bis 5 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.

(7) Absatz 1 und Absatz 2 Satz 1 und 5 sowie Absatz 5 finden keine Anwendung, soweit die zur Übermittlung vorgesehenen Daten mit schriftlicher Einwilligung derbetroffenen Personen zum Zwecke der Übermittlung im automatisierten Abrufverfahren gespeichert sind. § 4 Abs. 1 Satz 4 und 5 gilt entsprechend.

(8) Die Absätze 1 bis 7 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

§ 10
Technische und organisatorische Maßnahmen

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen.

(2) Dabei sind Maßnahmen zu treffen, 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),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzepts zu ermitteln, zu dessen Bestandteilen die Vorabkontrolle hinsichtlich möglicher Gefahren für das in § 1 geschützte Recht auf informationelle Selbstbestimmung gehört, die vor der Entscheidung über den Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens durchzuführen ist. Das Verfahren darf nur eingesetzt werden, wenn diese Gefahren nicht bestehen oder durch Maßnahmen nach den Absätzen 1 und 2 verhindert werden können. Das Ergebnis der Vorabkontrolle ist aufzuzeichnen. 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.

(4) Der Landesrechnungshof kann von der zu prüfenden Stelle verlangen, dass für ein konkretes Prüfungsverfahren die notwendigen Maßnahmen nach den Absätzen 1 bis 3 zeitnah geschaffen werden.

§ 10 a

Datenschutzaudit

Die öffentlichen Stellen können zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größtmöglicher Datensparsamkeit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Sie können auch bereits geprüfte und bewertete Datenschutzkonzepte und Programme zum Einsatz bringen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 11

Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle verarbeitet, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftraggeber ist verantwortliche Stelle im Sinne dieses Gesetzes; die in § 5 genannten Rechte sind ihm gegenüber geltend zu machen. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach § 10 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

(2) Soweit das Landesamt für Datenverarbeitung und Statistik (Landesdatenverarbeitungszentrale), die Gemeinsamen Gebietsrechenzentren, die Fachrechenzentren, die Hochschulrechenzentren und die kommunalen Datenverarbeitungseinrichtungen personenbezogene Daten im Auftrag öffentlicher Stellen verarbeiten, gelten für sie außer §§ 6 und 10 auch § 22 sowie §§ 24 und 25 dieses Gesetzes unmittelbar.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs dieses Gesetzes ist die zuständige Datenschutzkontrollbehörde zu unterrichten.

(4) Externe Personen und Stellen, die mit der Wartung und Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung beauftragt sind, unterliegen den Regelungen der Datenverarbeitung im Auftrag. Sie müssen die no twendige 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 Auftrages zu löschen. Die Dokumentation der Maßnahmen ist zum Zweck der Datenschutzkontrolle drei Jahre aufzubewahren.

Zweiter Abschnitt Rechtsgrundlagen der Datenverarbeitung

§ 12

Erhebung

(1) Das Erheben personenbezogener Daten ist nur insoweit zulässig, als ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Durch die Art und Weise der Erhebung darf das allgemeine Persönlichkeitsrecht der betroffenen Person nicht beeinträchtigt werden.
Personenbezogene Daten sind bei der betroffenen Person mit ihrer Kenntnis zu erheben; bei anderen Stellen oder Personen dürfen sie ohne ihre Kenntnis nur unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstabe a und c bis g oder i erhoben werden.

(2) Werden Daten bei der betroffenen Person erhoben, so ist sie über den Verwendungszweck und eine etwaige beabsichtigte Übermittlung aufzuklären. Werden Daten aufgrund einer Rechtsvorschrift erhoben, so ist die betroffene Person in geeigneter Weise über diese aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechtsvorteilen sind, ist die betroffene Person hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Werden Daten ohne Kenntnis der betroffenen Person erstmals erhoben, so ist sie bei Beginn der Speicherung oder im Fall einer vorgesehenen Übermittlung bei der erstenÜbermittlung davon zu benachrichtigen, wenn die Erfüllung der Aufgaben dadurch nicht wesentlich beeinträchtigt wird. Satz 4 gilt nicht, wenn die betroffene Person auf andere Weise Kenntnis erhält, die Übermittlung durch Gesetz oder eine andere Rechtsvorschrift ausdrücklich vorgesehen ist oder die Daten für Zwecke von Statistiken, die durch Gesetz oder eine andere Rechtsvorschrift vorgeschrieben sind, verarbeitet werden. Mitzuteilen ist, welche Daten von welcher Stelle zu welchem Zweck auf welcher Rechtsgrundlage erhoben oder an wen sie übermittelt worden sind.

(3) Werden Daten bei einer dritten Person oder einer nicht-öffentlichen Stelle erhoben, so ist diese auf Verlangen über den Verwendungszweck aufzuklären. Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 13
Zweckbindung bei Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Die Daten dürfen nur für Zwecke weiterverarbeitet werden, für die sie erhoben worden sind. Daten, von denen die Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder erstmals gespeichert worden sind, ist dies nur zulässig, wenn

a. eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt,
b. die betroffene Person eingewilligt hat,
c. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
d. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr
e. einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist, die Einholung der Einwilligung der betroffenen Person nicht möglich ist oder mit unverhältnismäßig hohem Aufwand verbunden wäre, aber offensichtlich ist, dass es in ihrem Interesse liegt und sie in Kenntnis des anderen Zwecks ihre Einwilligung erteilen würde,
f. sie aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, dass das Interesse der betroffenen Person an dem Ausschluss der Speicherung oder einer Veröffentlichung der gespeicherten Daten offensichtlich überwiegt,
g. es zu Zwecken einer öffentlichen Auszeichnung oder Ehrung der betroffenen Person erforderlich ist,
h. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint oder
i. zur Durchsetzung öffentlich-rechtlicher Geldforderungen ein rechtliches Interesse an der Kenntnis der zu verarbeitenden Daten vorliegt und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung überwiegt.

Die betroffene Person ist außer im Fall des Buchstaben b davon in geeigneter Weise zu unterrichten, sofern nicht die Aufgabenerfüllung wesentlich beeinträchtigt wird. 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, findet Satz 1 Buchstabe c bis i keine Anwendung.

(3) Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwecken, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten offensichtlich überwiegen.

§ 14

Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Voraussetzungen des § 13 Abs. 1 Satz 2 oder Satz 3 oder des Absatzes 2 Satz 1 vorliegen, sowie zur Wahrnehmung von Aufgaben nach § 13 Abs. 3. Die Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

(2) Die Verantwortung für die Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Grund eines Ersuchens des Empfängers, hat die übermittelnde Stelle lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; der Empfänger hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf (§ 9), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

(3) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu deren Erfüllung sie ihm übermittelt worden sind; § 13 Abs. 2 findet entsprechende Anwendung.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 15

Übermittlung an öffentlich-rechtliche Religionsgesellschaften

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.

§ 16

Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

a. sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des § 13 Abs. 1 vorliegen,
b. die Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstabe a, b, d, f oder i vorliegen,
c. der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das Geheimhaltungsinteresse der betroffenen Person überwiegt, oder
d. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die betroffene Person in diesen Fällen der Datenübermittlung nicht widersprochen hat.

Bei Übermittlungen nach Satz 1 Buchstabe b, soweit sie unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstabe i erfolgen, sowie in den Fällen des Satzes 1 Buchstabe c wird die betroffene Person vor der Mitteilung gehört, es sei denn, es ist zu besorgen, dass dadurch die Verfolgung des Interesses vereitelt oder wesentlich erschwert würde, und eine Abwägung ergibt, dass dieses Interesse das Interesse der betroffenen Person an ihrer vorherigen Anhörung überwiegt; ist die Anhörung unterblieben, wird die betroffene Person nachträglich unterrichtet. In den übrigen Fällen des Satzes 1 ist die betroffene Person über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten, sofern nicht die Aufgabenerfüllung wesentlich beeinträchtigt wird.

(2) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu denen sie ihm übermittelt wurden. Hierauf ist er bei der Übermittlung hinzuweisen.

§ 17

Übermittlung an ausländische Stellen

(1) Die Zulässigkeit der Übermittlung an öffentliche und nicht-öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes richtet sich nach den §§ 14 und 16. Die Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Vor der Entscheidung über die Angemessenheit des Datenschutzniveaus ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zu hören.

(2) Fehlt es an einem angemessenen Datenschutzniveau, so ist die Übermittlung nur zulässig, wenn

1. die betroffene Person in die Übermittlung eingewilligt hat,
2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,

3. die Übermittlung zur Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist,
4. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt oder
5. die Übermittlung genehmigt wird, wenn die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der informationellen Selbstbestimmung bietet. Die für die Genehmigungserteilung zuständige Stelle oder zuständigen Stellen bestimmt die Landesregierung durch Rechtsverordnung.

(3) Die empfangende Stelle ist darauf hinzuweisen, dass die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

Dritter Abschnitt Rechte der betroffenen Person

§ 18
Auskunft, Einsichtnahme

(1) Der betroffenen Person ist von der verantwortlichen Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person verarbeiteten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie
4. die allgemeinen technischen Bedingungen der automatisierten Verarbeitung der zur eigenen Person verarbeiteten Daten.

Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(2) Auskunft oder Einsichtnahme sind zu gewähren, soweit die betroffene Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen. Auskunftserteilungen und Einsichtnahme sind gebührenfrei, die Erstattung von Auslagen kann verlangt werden.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Einsichtnahme entfällt, soweit

a. dies die ordnungsgemäße Erfüllung der Aufgaben der verantwortlichen Stelle erheblich gefährden würde,
b. dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
c. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) Einer Begründung für die Auskunftsverweigerung bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

(5) Bezieht sich die Auskunftserteilung oder die Einsichtnahme auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 19 Abs. 3 Bundesdatenschutzgesetz genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 3 und 4 entsprechend.

(6) Werden Auskunft oder Einsichtnahme nicht gewährt, ist die betroffene Person darauf hinzuweisen, dass sie sich an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden kann.

§ 19

Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten zu berichtigen, so ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig wa ren oder geworden sind.

(2) Personenbezogene Daten sind zu sperren, wenn

a. ihre Richtigkeit von der betroffenen Person bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
b. die betroffene Person an Stelle der Löschung nach Absatz 3 Satz 1 Buchstabe a die Sperrung verlangt,

c. die weitere Speicherung im Interesse der betroffenen Person geboten ist,
d. sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

In den Fällen nach Satz 1 Buchstabe c und d sind die Gründe aufzuzeichnen. Bei automatisierten Dateien ist die Sperrung grundsätzlich durch technische Maßnahmensicherzustellen; im Übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr weiterverarbeitet

werden, es sei denn, dass dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder die betroffene Person eingewilligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn

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

Sind personenbezogene Daten in Akten gespeichert und ist die nach § 4 Abs. 6 vorgesehene Abtrennung nicht möglich, ist die Löschung nach Satz 1 Buchstabe b 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.

(4) Abgesehen von den Fällen des Absatzes 3 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten auf Grund von Rechtsvorschriften einem Archiv zur Übernahme anzubieten oder von einem Archiv zu übernehmen sind.

(5) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die betroffene Person und die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für die betroffene Person nicht zu befürchten sind.

§ 20

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, so ist ihr der Träger der verantwortlichen Stelle zum Schadensersatz verpflichtet. In schweren Fällen kann die betroffene Person auch wegen des Schadens, der nicht Vermögensschaden ist, eine angemessene Entschädigung in Geld verlangen.

(2) Ist der Schaden durch Verarbeitung der Daten in einer automatisierten Datei entstanden, besteht die Entschädigungspflicht unabhängig von einem Verschulden der verantwortlichen Stelle. In diesem Fall haftet der Ersatzpflichtige gegenüber der betroffenen Person für jedes schädigende Ereignis bis zu einem Betrag von 500.000 Deutsche Mark oder 250.000 Euro. Im Übrigen setzt die Verpflichtung zum

Schadensersatz Verschulden voraus. Der verantwortlichen Stelle obliegt in Fällen des Satzes 3 die Beweislast, dass sie die unzulässige oder unrichtige Verarbeitung der Daten nicht zu vertreten hat. Mehrere Ersatzpflichtige haften als Gesamtschuldner.

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

(4) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

§ 21
Berufung und Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung einen Landesbeauftragten für Datenschutz und Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Dieser muss die Befähigung zum Richteramt oder zum höheren Dienst haben und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde besitzen. Die Amts- und Funktionsbezeichnung "Landesbeauftragter für Datenschutz und Informationsfreiheit" wird in männlicher oder weiblicher Form geführt.

(2) Der Landesbeauftragte für Datenschutz und Informationsfreiheit wird jeweils für die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. Nach Ende der Amtszeit bleibt er bis zur Ernennung eines Nachfolgers im Amt. Die Wiederwahl ist zulässig. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit bestellt eine Mitarbeiterin oder einen Mitarbeiter zur Stellvertreterin oder zum Stellvertreter. Diese oder dieser führt die Geschäfte im Verhinderungsfall.

(3) Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist dem Innenministerium angegliedert. Er ist oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung und trifft Entscheidungen nach §§ 64 und 65 des Landesbeamtengesetzes für das Land Nordrhein-Westfalen für sich und seine Bediensteten in eigener Verantwortung. Im Übrigen untersteht er der Dienstaufsicht des Innenministeriums.

(4) Dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Innenministeriums in einem eigenen Kapitel auszuweisen.

(5) In Personalangelegenheiten hat der Landesbeauftragte für Datenschutz und Informationsfreiheit ein Vorschlagsrecht. Die Stellen sind im Einvernehmen mit ihm zu besetzen. Die Bediensteten können nur im Einvernehmen mit ihm versetzt oder abgeordnet werden; sie unterstehen seinen Weisungen.

(6) Der Landesbeauftragte für Datenschutz und Informationsfreiheit kann sich jederzeit an den Landtag wenden.

§ 22

Aufgaben und Befugnisse

(1) Der Landesbeauftragte für Datenschutz und Informationsfreiheit überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen. Den Stellen kann der Landesbeauftragte für Datenschutz und Informationsfreiheit auch Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere die Landesregierung und einzelne Ministerien, Gemeinden und Gemeindeverbände sowie die übrigen öffentlichen Stellen in Fragen des Datenschutzes beraten.

(2) Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für Datenschutz und Informationsfreiheit bei der Aufgabenerfüllung zu unterstützen und Amtshilfe zu leisten. Gesetzliche Geheimhaltungsvorschriften können einem Auskunfts- oder Einsichtsverlangen nicht entgegengehalten werden. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit sind insbesondere

1. Auskunft über die Fragen zu erteilen sowie Einsicht in alle Datenverarbeitungsvorgänge, Dokumentationen und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich auch in die gespeicherten Daten,
2. jederzeit Zutritt zu allen Diensträumen und Zugriff auf elektronische Dienste zu gewähren und
3. Kopien von Unterlagen, von automatisierten Dateien, von deren Verfahren und von organisatorischen Regelungen zur Mitnahme zur Verfügung zu stellen, soweit nicht die Aufgabenerfüllung der verantwortlichen Stelle wesentlich gefährdet wird. Die Gefährdung ist schriftlich zu begründen.

Die Rechte nach Satz 3 dürfen nur vom Landesbeauftragten für Datenschutz und Informationsfreiheit 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 ihm gegenüber nicht offenbart werden.

(3) 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. Dasselbe

gilt bei Entwürfen für Rechts- oder Verwaltungsvorschriften des Landes, wenn sie eine Verarbeitung personenbezogener Daten vorsehen.

(4) Der Landtag und die Landesregierung können den Landesbeauftragten für Datenschutz und Informationsfreiheit mit der Erstattung von Gutachten und Stellungnahmen oder der Durchführung von Untersuchungen in Datenschutzfragen betrauen.

(5) Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist befugt, personenbezogene Daten, die ihm durch Beschwerden, Anfragen, Hinweise und Beratungswünsche bekannt werden, zu verarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. 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. Die nach den Sätzen 1 und 2 erhobenen und verarbeiteten Daten dürfen nicht zu anderen Zwecken weiterverarbeitet werden.

(6) Der Landesbeauftragte für Datenschutz und Informationsfreiheit arbeitet mit den Behörden und sonstigen Stellen zusammen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in der Europäischen Union, im Bund und in den Ländern zuständig sind. Aufsichtsbehörde im Sinne des § 38 Bundesdatenschutzgesetz ist der Landesbeauftragte für Datenschutz und Informationsfreiheit. Insofern untersteht er der Aufsicht des Innenministeriums. Führt er die Weisungen nicht aus, kann ihn das Innenministerium erneut anweisen. Kommt er der neuerlichen Weisung nicht binnen einer Woche nach, steht zur Prüfung der Rechtmäßigkeit der Weisung der Rechtsweg vor dem Verwaltungsgericht offen. Kommt der Landesbeauftragte für Datenschutz und Informationsfreiheit der Weisung auch nach Bestätigung ihrer Rechtmäßigkeit durch das Verwaltungsgericht nicht nach, kann das Innenministerium den Vertreter anweisen; entgegenstehende Weisungen des Landesbeauftragten für Datenschutz und Informationsfreiheit sind unbeachtlich. Das Innenministerium und der Landesbeauftragte für Datenschutz und Informationsfreiheit werden ermächtigt, Regelungen zum weiteren Verfahren der Aufsicht im nicht-öffentlichen Bereich zu vereinbaren.

§ 23

(aufgehoben)

§ 24

Beanstandungen durch den Landesbeauftragten

(1) Stellt der Landesbeauftragte für Datenschutz und Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes, gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde, beim Landesrechnungshof gegenüber der Präsidentin oder dem Präsidenten,
2. bei der Kommunalverwaltung gegenüber der jeweils verantwortlichen Gemeinde oder dem verantwortlichen Gemeindeverband,

3. bei den wissenschaftlichen Hochschulen, Gesamthochschulen und Fachhochschulen gegenüber dem Hochschulpräsidenten oder dem Rektor, bei öffentlichen Schulen gegenüber dem Leiter der Schule,
4. 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 ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 bis 4 unterrichtet der Landesbeauftragte für Datenschutz und Informationsfreiheit gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) 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.

(3) Mit der Beanstandung kann der Landesbeauftragte für Datenschutz und Informationsfreiheit Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die in Absatz 1 Nr. 2 bis 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für Datenschutz und Informationsfreiheit zu.

§ 25

Anrufungsrecht der betroffenen Person

(1) Wer der Ansicht ist, dass gegen Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht, hat das Recht, sich unmittelbar an den Landesbeauftragten für Datenschutz und Informationsfreiheit zu wenden; dies gilt auch für Bedienstete öffentlicher Stellen, ohne dass der Dienstweg eingehalten werden muss.
(2) Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den

Landesbeauftragten für Datenschutz und Informationsfreiheit wendet.

§ 26

(aufgehoben)

§ 27

Datenschutzbericht

Der Landesbeauftragte für Datenschutz und Informationsfreiheit legt dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über seine Tätigkeit vor (Datenschutzbericht). Die Landesregierung nimmt hierzu gegenüber dem Landtag schriftlich Stellung. Der Landesbeauftragte für Datenschutz und Informationsfreiheit berät und informiert mit dem Bericht und auf andere Weise die Bürger sowie die Öffentlichkeit zu Fragen des Datenschutzes.

Dritter Teil Besonderer Datenschutz

§ 28
Datenverarbeitung für wissenschaftliche Zwecke

(1) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen 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 dürfen personenbezogene Daten für ein bestimmtes Forschungsvorhaben verarbeitet werden, wenn

1. die betroffene Person eingewilligt hat,

2. schutzwürdige Belange der betroffenen Person wegen der Art der Daten oder der Art der Verwendung nicht beeinträchtigt werden oder
3. der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßig großem Aufwand erreicht werden kann und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Person überwiegt.

(3) Sobald es der Forschungszweck gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. Die Merkmale, mit deren Hilfe ein Personenbezug wiederhergestellt werden kann, sind gesondert zu speichern; sie müssen gelöscht werden, sobald der Forschungszweck dies zulässt. Sollen personenbezogene Daten für einen anderen als den ursprünglichen Forschungszweck verarbeitet werden, ist dies nur nach Maßgabe der Absätze 1 und 2 zulässig.

(4) Die zu wissenschaftlichen Zwecken verarbeiteten Daten dürfen nur veröffentlicht werden, wenn

1. die betroffene Person eingewilligt hat oder
2. das öffentliche Interesse an der Darstellung des Forschungsergebnisses die schutzwürdigen Belange der betroffenen Person erheblich überwiegt.

(5) Soweit öffentliche Stellen personenbezogene Daten übermitteln, haben sie diejenigen empfangenden Stellen, auf die dieses Gesetz keine Anwendung findet, darauf zu verpflichten, die Vorschriften der Absätze 1 bis 4 einzuhalten und jederzeit Kontrollen durch 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.

§ 29

Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Daten von Bewerbern und Beschäftigten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Abweichend von § 16 Abs. 1 ist eineÜbermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs 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) Die beamtenrechtlichen Vorschriften über die Führung von Personalakten (§§ 102 ff. Landesbeamtengesetz) 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.

(3) Die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses erhobenen Daten ist nur mit schriftlicher Einwilligung der betroffenen Person zulässig. Die Einstellungsbehörde darf vom untersuchenden Arzt in der Regel nur dieÜbermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen.

(4) Personenbezogene Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses 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. Nach Beendigung eines Dienst- oder Arbeitsverhältnisses sind personenbezogene Daten zu löschen, wenn diese Daten nicht mehr benötigt werden, es sei denn, dass Rechtsvorschriften entgegenstehen; § 19 Abs. 3 Satz 2 und 3 sowie Abs. 4 finden Anwendung.

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

(6) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

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

§ 29 a

Mobile personenbezogene Datenverarbeitungssysteme

(1) Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme, z. B. Chipkarten), dürfen nur mit Einwilligung der betroffenen Person nach ihrer vorherigen umfassenden Aufklärung eingesetzt werden.

(2) Für die Betroffenen muss jederzeit erkennbar sein,

1. ob und durch wen Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst stattfinden,

2. welche personenbezogenen Daten der betroffenen Person verarbeitet werden und
3. welcher Verarbeitungsvorgang im Einzelnen abläuft oder angestoßen wird.

Den Betroffenen müssen die Informationen nach Nummer 2 und 3 auf ihren Wunsch auch schriftlich in Papierform mitgeteilt werden.

(3) Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach § 5 zustehenden Rechte aufzuklären. Sofern zur Wahrnehmung der Informationsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür Sorge zu tragen, dass diese in angemessenem Umfang zur Verfügung stehen.

§ 29 b

Optisch-elektronische Überwachung

(1) Die nicht mit einer Speicherung verbundene Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen ist zulässig, soweit dies der Wahrnehmung des Hausrechts dient und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen. Die Tatsache der Beobachtung ist, soweit nicht offenkundig, den Betroffenen durch geeignete Maßnahmen erkennbar zu machen.

(2) Die Speicherung von nach Absatz 1 Satz 1 erhobenen Daten ist nur bei einer konkreten Gefahr zu Beweiszwecken zulässig, wenn dies zum Erreichen der verfolgten Zwecke unverzichtbar ist. Die Daten sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind; dies ist in angemessenen Zeitabständen zu prüfen.

(3) Werden die gespeicherten Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese jeweils davon zu benachrichtigen. Von einer Benachrichtigung kann abgesehen werden, solange das öffentliche Interesse an einer Strafverfolgung das Benachrichtigungsrecht der betroffenen Person erheblich überwiegt.

§ 30

Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn die betroffene Person zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlicheingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung

dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn die betroffene Person erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist; dies gilt nicht für Fernmess-und Fernwirkdienste der Versorgungsunternehmen. Die betroffene Person kann ihre Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass die betroffene Person nach Absatz 1 Satz 1 oder 2 einwilligt. Verweigert oder widerruft sie ihre Einwilligung, so dürfen ihr keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmess- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 31

Nutzung von Verwaltungsdaten für die Erstellung von Statistiken

Für die Erstellung von Statistiken dürfen öffentliche Stellen personenbezogene Daten weiterverarbeiten, soweit diese bei der rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben angefallen sind. Die Veröffentlichungen dürfen keine Angaben enthalten, die den Bezug auf eine bestimmte Person zulassen.

§ 32

Nutzung von Einzelangaben aus der amtlichen Statistik durch Gemeinden und Gemeindeverbände

(1) Dürfen den Gemeinden und Gemeindeverbänden auf Grund gesetzlicher Ermächtigungen zur Durchführung eigener statistischer Aufgaben Einzelangaben aus der amtlichen Statistik (Datensätze) für ihren Zuständigkeitsbereich übermittelt werden, so ist dies nur zulässig auf Datenträgern, die zur maschinellen Weiterverarbeitung bestimmt sind.

(2) Datenträger dürfen nur den für die Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände übermittelt werden, die organisatorisch und räumlich von den anderen Verwaltungsstellen der Körperschaft getrennt, gegen den Zutritt unbefugter Personen hinreichend geschützt und mit eigenem Personal ausgestattet sind, das die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet, schriftlich auf das Statistikgeheimnis verpflichtet worden

und während der Tätigkeit in der Statistikdienststelle nicht mit anderen Aufgaben des Verwaltungsvollzuges betraut ist.

(3) Die in den Statistikdienststellen der Gemeinden und Gemeindeverbände tätigen Personen dürfen die aus den nach Absatz 1 übermittelten Einzelangaben gewonnenen personenbezogenen Erkenntnisse während und nach ihrer Tätigkeit in der Statistikdienststelle nicht in anderen Verfahren oder für andere Zwecke verarbeiten oder offenbaren.

(4) Eine Durchführung eigener statistischer Aufgaben im Sinne des Absatzes 1 liegt nur vor, wenn aus den übermittelten Einzelangaben auf Grund vorgegebener sachlicher Kriterien Zahlensummen (Tabellen) erstellt werden, aus denen kein Bezug auf eine bestimmte Person hergestellt werden kann. Die Speicherung der übermittelten Einzelangaben in Dateien für andere als statistische Nutzungen und ihre Zusammenführung mit anderen Einzelangaben, aus denen ein Bezug zu personenbezogenen Daten hergestellt werden kann, sind unzulässig.

(5) Die Übermittlung nach Absatz 1 ist nach Zeitpunkt, Art der übermittelten Daten, Zweck der Übermittlung und Empfänger von der übermittelnden Dienststelle, nach Art und Zeitpunkt der Nutzung von der Dienststelle, die die Daten erhalten hat, aufzuzeichnen. Die Aufzeichnungen sind fünf Jahre aufzubewahren.

§ 32 a

Behördliche Datenschutzbeauftragte

(1) Öffentliche Stellen, die personenbezogene Daten verarbeiten, haben einen internen Beauftragten für Datenschutz sowie einen Vertreter zu bestellen. Der Beauftragte muss die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Mehrere Stellen können gemeinsam einen Beauftragten für Datenschutz bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird. Bei Bedarf kann eine Stelle auch mehrere Beauftragte sowie mehrere Vertreter bestellen. Der Beauftragte unterstützt die Stelle bei der Sicherstellung des Datenschutzes. Er berät die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten und überwacht bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren die Einhaltung der einschlägigen Vorschriften. Er ist bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten frühzeitig zu beteiligen und hat die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen und die Vorabkontrolle durchzuführen. Satz 5 findet auch Anwendung auf die Tätigkeit von Personalvertretungen, soweit bei diesen personenbezogene Daten verarbeitet werden.

(2) Der Beauftragte ist in seiner Eigenschaft als behördlicher Datenschutzbeauftragter

der Leitung der öffentlichen Stelle unmittelbar zu unterstellen und in dieser Funktion weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Während seiner Tätigkeit darf er mit keiner Aufgabe betraut sein, deren Wahrnehmung zu Interessenkollision führen könnte.

(3) Die verantwortliche Stelle ist verpflichtet, dem Beauftragten die Beschreibung aller automatisiert geführten Verfahren, in denen personenbezogene Daten verarbeitet werden, mit den nach § 8 Abs. 1 vorgesehenen Angaben vorzulegen. Der Beauftragte führt das Verfahrensverzeichnis. Er gewährt jeder Person unentgeltlich nach Maßgabe des § 8 Abs. 2 Einsicht in das Verfahrensverzeichnis. Das Einsichtsrecht in die Verfahrensverzeichnisse, die bei den in § 2 Abs. 2 Satz 1 genannten Stellen geführt werden, kann verwehrt werden, soweit damit Betriebs oder Geschäftsgeheimnisse offenbart würden. Wird keine Einsicht gewährt, ist in geeigneter Weise Auskunft zu erteilen; die Gründe für die Verweigerung der Einsichtnahme sind aktenkundig zu machen und die einsichtverlangende Person ist darauf hinzuweisen, dass sie sich an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden kann. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit ist auf sein Verlangen Einsicht in das Verfahrensverzeichnis zu gewähren.

(4) Bedienstete der öffentlichen Stellen können sich jederzeit in Angelegenheiten des Datenschutzes unmittelbar an den Beauftragten wenden. Der Beauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf diese zulassen, verpflichtet, soweit er von der betroffenen Person davon nicht befreit wurde.

Vierter Teil
Straf- und Bußgeldvorschriften; Übergangsvorschriften
§ 33
Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, 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. Der Versuch ist strafbar.

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

§ 34

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre 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 100.000 Deutschen Mark oder 50.000 Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist für die Verfolgung und Ahndung von Ordnungswidrigkeiten

a. nach den Absätzen 1 und 2 die Bezirksregierung,
b. nach § 43 des Bundesdatenschutzgesetzes und nach § 9 des Teledienstedatenschutzgesetzes der Landesbeauftragte für Datenschutz und Informationsfreiheit.

§ 35

Übergangsvorschriften

(1) Verarbeitungen personenbezogener Daten, die zum Zeitpunkt des In-Kraft-Tretens dieses Gesetzes[1] bereits begonnen wurden, sind innerhalb von drei Jahrennach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

(2) Für Behörden des Justizvollzuges gilt § 18 mit der Maßgabe, dass die betroffene Person Auskunft oder Akteneinsicht erhält, soweit sie zur Wahrnehmung ihrer Rechte oder berechtigten Interessen auf die Kenntnis gespeicherter Daten angewiesen ist. § 185 des Strafvollzugsgesetzes bleibt unberührt.

(3) Für Dateien, die bereits zum Register des Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet sind, finden die Vorschriften des § 8 Abs. 1 und des § 32 a Abs. 3 erstmals in Fällen eintretender Veränderungen Anwendung. Im Übrigen wird die Dateienregisterverordnung vom 11. April 1989 (GV. NRW. S. 226) aufgehoben.

§ 36

Berichtspflicht

Die Landesregierung berichtet dem Landtag bis zum 31. Dezember 2009 über die Erfahrungen mit diesem Gesetz.

[1] Dies bezieht sich auf das Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NW) vom 9. Mai 2000 (GV. NRW. S. 452), in Kraft getreten am 31. Mai 2000.