Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) Vom 25. August 2003 (SächsGVBl S. 329)

Der Sächsische Landtag hat am 10. Juli 2003 das folgende Gesetz beschlossen:[1]

Inhaltsübersicht

Abschnitt 1
Allgemeine Vorschriften

§ 1 Zweck des Gesetzes
§ 2 Anwendungsbereich
§ 3 Begriffsbestimmungen
§ 4 Zulässigkeit der Datenverarbeitung
§ 5 Rechte des Betroffenen
§ 6 Datengeheimnis
§ 7 Datenverarbeitung im Auftrag, Datenschutz bei Wartungsarbeiten
§ 8 Automatisiertes Abrufverfahren
§ 9 Maßnahmen zur Gewährleistung des Datenschutzes
§ 10 Verzeichnis automatisierter Verarbeitungsverfahren, Meldepflicht, Vorabkontrolle
§ 11 Datenschutzbeauftragte öffentlicher Stellen

Abschnitt 2
Rechtsgrundlagen der Datenverarbeitung

§ 12 Erhebung
§ 13 Speicherung, Veränderung und Nutzung
§ 14 Übermittlung an öffentliche Stellen
§ 15 Übermittlung an öffentlich-rechtliche Religionsgesellschaften
§ 16 Übermittlung an nicht-öffentliche Stellen
§ 17 Übermittlung in Drittländer

Abschnitt 3
Rechte des Betroffenen

§ 18 Auskunft
§ 19 Berichtigung
§ 20 Löschung
§ 21 Sperrung
§ 22 Widerspruchsrecht
§ 23 Schadensersatz
§ 24 Anrufung des Sächsischen Datenschutzbeauftragten

[1] Dieses Gesetz dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31).

Abschnitt 4
Sächsischer Datenschutzbeauftragter

§ 25 Berufung und Rechtsstellung
§ 26 Anhörung des Sächsischen Datenschutzbeauftragten
§ 27 Kontrolle durch den Sächsischen Datenschutzbeauftragten
§ 28 Pflicht zur Unterstützung
§ 29 Beanstandungen und sonstige Äußerungen
§ 30 Tätigkeitsbericht und weitere Aufgaben
§ 31 Datenschutzregister

Abschnitt 5
Sonstige Vorschriften

§ 32 Fernmessen und Fernwirken
§ 33 Videoüberwachung und Videoaufzeichnung
§ 34 Automatisierte Einzelentscheidungen
§ 35 Mobile personenbezogene Datenverarbeitungsmedien
§ 36 Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung
§ 37 Schutz von Beschäftigtendaten im öffentlichen Dienst
§ 38 Ordnungswidrigkeiten
§ 39 Straftaten
§ 40 Übergangsregelungen
§ 41 Einschränkung eines Grundrechts
§ 42 In-Kraft-Treten und Außer-Kraft-Treten

Abschnitt 1
Allgemeine Vorschriften

§ 1
Zweck des Gesetzes

Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er im Freistaat Sachsen durch Behörden und sonstige öffentliche Stellen bei der Verarbeitung personenbezogener Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Freistaates Sachsen, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen).

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Abs. 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Für den Sachsen-Finanzverband, die Sachsen-Finanzgruppe und die Sparkassen sowie für andere öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit, die am Wettbewerb teilnehmen, gelten die Vorschriften des Bundesdatenschutzgesetzes (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch Artikel 12 des Gesetzes vom 21. August 2002 (BGBl. I S. 3322, 3330), in der jeweils geltenden Fassung, mit Ausnahme des zweiten Abschnittes.

(4) Soweit besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes den Schutz personenbezogener Daten regeln, 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 (Betroffener).

(2) Verarbeiten ist das Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Erheben das Beschaffen von personenbezogenen Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
4. Anonymisieren das Verändern personenbezogener Daten in der Weise, dass sie nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können,
5. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, dass
   a) die Daten durch die datenverarbeitende Stelle an den Empfänger weitergegeben werden oder
   b) dieser zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
6. Nutzen jede sonstige Verwendung personenbezogener Daten,
7. Sperren die Einschränkung der weiteren Verarbeitung personenbezogener Daten,
8. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(3) Datenverarbeitende Stelle ist jede Stelle, die personenbezogene Daten für sich selbst oder für andere verarbeitet oder durch andere im Auftrag verarbeiten lässt.

(4) Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene und der Auftragnehmer im Sinne des § 7 im Verhältnis zu seinem Auftraggeber in Ausführung des konkreten Auftragsverhältnisses.

(5) Eine automatisierte Verarbeitung personenbezogener Daten liegt vor, wenn diese durch Einsatz eines elektronischen Datenverarbeitungssystems programmgesteuert durchgeführt wird.

(6) Eine Akte ist jeder amtlichen oder dienstlichen Zwecken dienende Träger personenbezogener Daten einschließlich Bild- und Tonträgern, soweit sie nicht im Sinne von Absatz 5 automatisiert verarbeitet werden.

(7) Soweit andere landesrechtliche Vorschriften den Dateibegriff im Zusammenhang mit der Verarbeitung personenbezogener Daten verwenden und nichts anderes bestimmen, ist eine Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder
2. eine andere Sammlung personenbezogener Daten, die nach bestimmten Merkmalen geordnet, umgeordnet oder ausgewertet werden kann (nicht-automatisierte Datei).

§ 4
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig,

1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. soweit der Betroffene eingewilligt hat.

(2) Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben, ist nur zulässig, wenn

1. aus Gründen eines wichtigen öffentlichen Interesses eine besondere Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss,
3. die Verarbeitung für den Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu erteilen, oder
4. offenkundig ist, dass der Betroffene die Daten selbst öffentlich zugänglich gemacht hat.

(3) Wer die Einwilligung des Betroffenen einholt, hat ihn zuvor in geeigneter Weise über die beabsichtigte Datenverarbeitung und ihren Zweck sowie die Empfänger vorgesehener Übermittlungen aufzuklären. Dabei ist er unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann, sofern dem Widerruf keine Rechtsgründe entgegenstehen.

(4) Die Einwilligung und die Hinweise bedürfen der Schriftform, soweit nicht im Einzelfall wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(5) Das Erfordernis der Schriftform für die Einwilligung nach Absatz 4 kann durch die mit einer qualifizierten elektronischen Signatur verbundene elektronische Form ersetzt werden. Die Signatur mit einem Pseudonym ersetzt nicht die Schriftform.

§ 5
Rechte des Betroffenen

(1) Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft über die zu seiner Person gespeicherten Daten (§ 18),
2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§§ 19 bis 21),
3. Widerspruch gegen die Verarbeitung seiner Daten (§ 22),
4. Schadensersatz (§ 23),
5. Anrufung des Sächsischen Datenschutzbeauftragten (§ 24),
6. Auskunft bei automatisierten Einzelentscheidungen (§ 34 Abs. 3).

(2) Die in Absatz 1 genannten Rechte können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(3) Sind an einer Verarbeitung der Daten des Betroffenen mehrere Stellen beteiligt, kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle weiterzuleiten, die seinem Begehren Rechnung tragen kann. Der Betroffene ist über die Weiterleitung zu unterrichten.

§ 6
Datengeheimnis

(1) Den für eine öffentliche Stelle tätigen Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(2) Die in Absatz 1 Satz 1 genannten Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung schriftlich zu verpflichten.

§ 7
Datenverarbeitung im Auftrag, Datenschutz bei Wartungsarbeiten

(1) Eine öffentliche Stelle kann, soweit gesetzlich nichts anderes bestimmt ist, einen anderen mit der Verarbeitung personenbezogener Daten beauftragen (Datenverarbeitung im Auftrag). Für die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz ist sowohl der Auftraggeber als auch der Auftragnehmer verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Gegenstand und Umfang der Datenverarbeitung, die notwendigen zusätzlichen personellen, technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, sich von der Einhaltung der getroffenen Festlegungen beim Auftragnehmer zu überzeugen. Der Auftraggeber hat dem Auftragnehmer die erforderlichen Weisungen zu erteilen. Die Datenverarbeitung ist nur im Rahmen des Auftrags und der Weisungen zulässig. Ist der Auftragnehmer der Ansicht, dass der Auftrag, eine einzelne Bestimmung des Auftrags oder eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(3) Ist der Auftragnehmer keine öffentliche Stelle im Sinne dieses Gesetzes, hat der Auftraggeber die für den Auftragnehmer zuständige Kontrollbehörde über die Beauftragung zu unterrichten.

(4) Die Beauftragung eines Auftragnehmers, der seinen Sitz außerhalb der Europäischen Union hat, ist nur zulässig, wenn eine Übermittlung an ihn nach § 17 Abs. 1 zulässig wäre. § 17 Abs. 4 gilt entsprechend.

(5) Die Absätze 1 bis 4 gelten für Wartungs- und Fernwartungsaufträge sowie ähnliche Maßnahmen (Wartungsarbeiten) entsprechend.

§ 8
Automatisiertes Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten an Dritte durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Die Zulässigkeit des einzelnen Abrufs beurteilt sich nach den für die Erhebung und Übermittlung geltenden Vorschriften. Die Verantwortung für die Zulässigkeit der Übermittlung im Einzelfall trägt die abrufende Stelle. Die Stelle, die die Daten für den Abruf bereithält, prüft die Zulässigkeit des Abrufes nur, wenn dazu Anlass besteht. Sie hat zu gewährleisten, dass die Zulässigkeit der Übermittlung personenbezogener Daten zumindest stichprobenweise überprüft werden kann.

(3) Die Stelle, die die Daten für den Abruf bereithält, führt das Verzeichnis nach § 10.

(4) Absatz 1 gilt nicht für Datenbestände, die der Allgemeinheit zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

§ 9
Maßnahmen zur Gewährleistung des Datenschutzes

(1) Öffentliche Stellen, die personenbezogene Daten verarbeiten, haben alle personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind nach dem jeweiligen Stand der Technik 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 (Authenzität),
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 Staatsregierung wird ermächtigt, durch Rechtsverordnung die in den Absätzen 1 und 2 genannten Anforderungen und Maßnahmen nach dem jeweiligen Stand der Technik näher zu bestimmen und fortzuschreiben.

(4) Werden personenbezogene Daten in Akten verarbeitet, sind besondere Maßnahmen zu treffen, um zu verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können.

§ 10
Verzeichnis automatisierter Verarbeitungsverfahren, Meldepflicht, Vorabkontrolle

(1) Jede datenverarbeitende Stelle führt ein Verzeichnis der bei ihr eingesetzten automatisierten Verarbeitungsverfahren. In dem Verzeichnis sind schriftlich festzulegen:

1. die Bezeichnung und die Anschrift der datenverarbeitenden Stelle,
2. die Bezeichnung des Verfahrens und dessen Zweckbestimmung,
3. die Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden und die Rechtsgrundlage der Verarbeitung,
4. die Art der zu verarbeitenden Daten,
5. der Kreis der Betroffenen,
6. die Art der zu übermittelnden Daten und die Empfänger der Daten,
7. die beabsichtigte Übermittlung in Drittländer gemäß § 17,
8. die personellen, technischen und organisatorischen Maßnahmen gemäß § 9.

Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach durchgeführt werden, können die Festlegungen zusammengefasst werden.

(2) Die Gerichte führen Verzeichnisse nach Absatz 1 nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden.

(3) Die datenverarbeitenden Stellen sind verpflichtet, dem Sächsischen Datenschutzbeauftragten vor dem erstmaligen Einsatz eines automatisierten Verarbeitungsverfahrens das Verzeichnis im Sinne des Absatzes 1 zuzuleiten. Die datenverarbeitende Stelle bringt das von ihr geführte Verzeichnis regelmäßig auf den neuesten Stand und leitet das aktualisierte Verzeichnis jährlich zum 1. März dem Sächsischen Datenschutzbeauftragten zu. Bei der Bestellung eines Datenschutzbeauftragten nach § 11 entfällt die Pflicht zur Zuleitung an den Sächsischen Datenschutzbeauftragten.

(4) Die Absätze 1 bis 3 gelten nicht für Verfahren,

1. deren einziger Zweck das Führen eines durch Rechtsvorschrift vorgeschriebenen Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, oder
2. die ausschließlich der Unterstützung der allgemeinen Bürotätigkeit dienen, insbesondere Verfahren der Textverarbeitung, Vorgangsverwaltung, Terminüberwachung und der

Führung von Adress-, Telefon- und vergleichbaren Verzeichnissen, soweit sie keine Beeinträchtigung der Rechte Betroffener erwarten lassen.

(5) Vor dem erstmaligen Einsatz oder der wesentlichen Änderung

1. eines Verfahrens nach § 8,
2. eines automatisierten Verfahrens, in dem Daten im Sinne des § 4 Abs. 2 verarbeitet werden oder
3. eines automatisierten Verfahrens, in dem Daten von Beschäftigten im Sinne des § 37 verarbeitet werden

ist durch den Sächsischen Datenschutzbeauftragten oder im Fall der Bestellung eines Datenschutzbeauftragten nach § 11 durch diesen zu prüfen, ob die Datenverarbeitung zulässig ist und die vorgesehenen Maßnahmen nach § 9 ausreichend sind (Vorabkontrolle). Die datenverarbeitende Stelle hat ihm dazu die erforderlichen Unterlagen zur Verfügung zu stellen. Die Stellungnahme soll innerhalb eines Monats abgegeben werden.

§ 11
Datenschutzbeauftragte öffentlicher Stellen

(1) Öffentliche Stellen im Sinne des § 2 Abs. 1 und 2 können einen Datenschutzbeauftragten bestellen. Die Bestellung bedarf der Schriftform. Mehrere öffentliche Stellen können gemeinsam einen Datenschutzbeauftragten bestellen. Der Datenschutzbeauftragte muss nicht Beschäftigter einer öffentlichen Stelle im Sinne dieses Gesetzes sein. § 25 Abs. 1 Satz 3 gilt entsprechend. Der Sächsische Datenschutzbeauftragte ist innerhalb eines Monats über die Bestellung zu unterrichten. Dabei sind der Name des Datenschutzbeauftragten sowie der Tag seiner Bestellung mitzuteilen. Hierüber führt der Sächsische Datenschutzbeauftragte ein Register.

(2) Zum Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Sachkunde und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit seinen sonstigen beruflichen Aufgaben ausgesetzt wird. Er ist bei der Erfüllung seiner Aufgaben dem Leiter der öffentlichen Stelle unmittelbar zu unterstellen und weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die öffentlichen Stellen haben den Datenschutzbeauftragten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, zu unterstützen und ihn im erforderlichen Umfang von der Erfüllung seiner sonstigen dienstlichen Pflichten freizustellen.

(3) Der Datenschutzbeauftragte hat die Aufgabe, die öffentliche Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Zu seinen Aufgaben gehört es insbesondere

1. die Einhaltung der Datenschutzvorschriften bei der Planung, Einführung und Anwendung von Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, zu überwachen,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz und den besonderen Erfordernissen des Datenschutzes in ihrem Tätigkeitsbereich vertraut zu machen,
3. für die öffentliche Stelle das Verzeichnis automatisierter Verarbeitungsverfahren (§ 10 Abs. 1) zu führen und regelmäßig auf den neuesten Stand zu bringen (§ 10 Abs. 3),

4. die Vorabkontrolle nach § 10 Abs. 5 durchzuführen; dabei hat er sich in Zweifelsfällen nach vorheriger Unterrichtung des Leiters der öffentlichen Stelle an den Sächsischen Datenschutzbeauftragten zu wenden,
5. auf Antrag im Einzelfall jedermann Auskunft über die Angaben nach § 10 Abs. 1 Satz 2 Nr. 1 bis 7 zu erteilen. Hiervon sind ausgenommen die Verzeichnisse der in § 18 Abs. 7 genannten Stellen. § 18 bleibt unberührt.

(4) Der Datenschutzbeauftragte ist, auch nach Beendigung seiner Tätigkeit, zur Verschwiegenheit über die Identität Betroffener und Beschäftigter, die sich an ihn gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, verpflichtet; § 6 bleibt unberührt. Dies gilt nicht, soweit die Betroffenen oder Beschäftigten ihn von der Pflicht zur Verschwiegenheit entbunden haben.

Abschnitt 2
Rechtsgrundlagen der Datenverarbeitung

§ 12
Erhebung

(1) Das Erheben personenbezogener Daten ist nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

(2) Personenbezogene Daten, die nicht allgemein zugänglich sind, sind beim Betroffenen mit seiner Kenntnis zu erheben. Dabei sind ihm zumindest Bezeichnung und Anschrift der erhebenden Stelle und gegebenenfalls des Auftragnehmers sowie der Erhebungszweck mitzuteilen. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die Folgen der Verweigerung von Angaben ist der Betroffene aufzuklären.

(3) Personenbezogene Daten, die nicht allgemein zugänglich sind, dürfen beim Betroffenen ohne seine Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt.

(4) Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn
1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass dies im Interesse des Betroffenen liegt, dieser nicht erreichbar ist und kein Grund zu der Annahme besteht, dass er seine Einwilligung hierzu verweigern würde,
4. der Betroffene einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen ist und über die beabsichtigte Erhebung bei Dritten unterrichtet worden ist,
5. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

7. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
8. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(5) Werden personenbezogene Daten bei einem Dritten außerhalb des öffentlichen Bereiches erhoben, ist dieser auf Verlangen auf den Erhebungszweck hinzuweisen, soweit dadurch schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, ist er auf die Auskunftspflicht, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die Folgen der Verweigerung von Angaben ist er aufzuklären.

(6) Werden personenbezogene Daten beim Betroffenen ohne seine Kenntnis oder bei Dritten erhoben, ist der Betroffene zu benachrichtigen. Dabei sind ihm zumindest Bezeichnung und Anschrift der erhebenden Stelle, die Rechtsgrundlage und der Erhebungszweck sowie bei einer beabsichtigten Übermittlung auch der Empfänger der Daten mitzuteilen. Die Mitteilung erfolgt zum Zeitpunkt der Speicherung oder im Fall einer beabsichtigten Übermittlung spätestens bei der ersten Übermittlung. Eine Pflicht zur Mitteilung besteht nicht, wenn

1. eine Auskunft nach § 18 Abs. 5 oder 7 unterbleiben würde,
2. eine Benachrichtigung des Betroffenen unmöglich ist,
3. eine Benachrichtigung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
4. die Speicherung oder Übermittlung durch Rechtsvorschrift vorgeschrieben ist.

(7) Absatz 6 gilt für Gerichte nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden.

§ 13
Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es

1. zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Daten nicht in unzulässiger Weise erhoben worden sind und
2. für Zwecke erfolgt, für die die Daten erhoben worden sind; ist keine Erhebung vorausgegangen, sind die Zwecke maßgebend, für die die Daten erstmalig gespeichert worden sind.

(2) Das Speichern, Verändern und Nutzen personenbezogener Daten für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, unter denen nach § 12 Abs. 4 eine Erhebung bei Dritten zulässig wäre,
2. die Daten allgemein zugänglich sind oder die datenverarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen,
3. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches (StGB) in der Fassung der Bekanntmachung vom 13. November 1998

(BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. Dezember 2002 (BGBl. I S. 3390), in der jeweils geltenden Fassung, oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes (JGG) in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch Artikel 3 des Gesetzes vom 19. Dezember 2000 (BGBl. I S. 1756), in der jeweils geltenden Fassung, oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

4. es zu historischen oder statistischen Zwecken erforderlich ist und das Interesse an der Durchführung des Vorhabens das Interesse des Betroffenen am Unterbleiben der Zweckänderung erheblich überwiegt; dies gilt nicht, wenn diese Zwecke auch durch die Verwendung anonymisierter Daten erreicht werden können, es sei denn, die Anonymisierung ist nicht oder nur mit unverhältnismäßigem Aufwand möglich, oder
5. dies für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist.

(3) Eine Speicherung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken der speichernden Stelle dient. Dies gilt auch für die Speicherung und Nutzung zu Ausbildungs- und Prüfungszwecken, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden.

(5) Sind mit personenbezogenen Daten, die nach den Absätzen 1 bis 3 gespeichert werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist die Speicherung auch dieser Daten zulässig, soweit nicht schutzwürdige Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen. Unter denselben Voraussetzungen dürfen die für die Aufgabenerfüllung nicht erforderlichen Daten innerhalb der speichernden Stelle weitergegeben werden; eine darüber hinausgehende Nutzung dieser Daten ist unzulässig.

(6) Die Zusammenführung von Daten zu Persönlichkeitsprofilen ist unzulässig.

§ 14
Übermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen im Sinne dieses Gesetzes, an öffentliche Stellen der anderen Länder, des Bundes, der Mitgliedstaaten der Europäischen Union sowie an Organe und Einrichtungen der Europäischen Union ist zulässig, wenn

1. sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 13 Abs. 1 bis 4 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(3) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 13 Abs. 2 zulässig. Unterliegen die übermittelten Daten einem Berufs- oder besonderen Amtsgeheimnis, ist ihre Verarbeitung für andere Zwecke nur zulässig, wenn die zur Verschwiegenheit verpflichtete Person oder Stelle eingewilligt hat.

(4) Für die Übermittlung verbundener Daten gilt § 13 Abs. 5 entsprechend.

§ 15
Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Für die Übermittlung personenbezogener Daten an öffentlich-rechtliche Religionsgesellschaften gilt § 14 entsprechend, sofern für den Empfänger ausreichende Datenschutzregelungen gelten. Die Feststellung hierüber trifft das Staatsministerium für Kultus im Einvernehmen mit dem Sächsischen Datenschutzbeauftragten.

§ 16
Übermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an natürliche Personen oder nicht-öffentliche Stellen in den Mitgliedstaaten der Europäischen Union ist zulässig, wenn

1. sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 13 Abs. 1 bis 4 zulassen würden, oder
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen des Absatzes 1 Nr. 2 ist der Betroffene vor der Übermittlung zu hören und im Falle der Übermittlung zu unterrichten; dies gilt nicht, wenn dem schwerwiegende öffentliche oder private Belange entgegenstehen.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt worden sind. Die übermittelnde Stelle hat den Empfänger hierauf hinzuweisen. Eine Verarbeitung für andere Zwecke ist nur zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle eingewilligt hat.

(5) Die übermittelnde Stelle kann die Übermittlung mit Auflagen versehen, die den Datenschutz beim Empfänger sicherstellen, oder mit diesem Vereinbarungen zur Gewährleistung des Datenschutzes treffen.

§ 17
Übermittlung in Drittländer

(1) Die Übermittlung personenbezogener Daten in anderen als den in §§ 14, 15 und 16 genannten Fällen ist unter den Voraussetzungen des § 16 Abs. 1 zulässig, wenn in dem Land, in das die Daten übermittelt werden (Drittland), ein angemessenes Datenschutzniveau gewährleistet ist.

(2) Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Bestimmungsland, die für den Empfänger geltenden Rechtsvorschriften sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(3) Fehlt es im Drittland an einem angemessenen Schutzniveau, ist die Übermittlung nur zulässig, wenn

1. der Betroffene eingewilligt hat,
2. die Übermittlung für die Erfüllung eines Vertrages zwischen dem Betroffenen und der datenverarbeitenden Stelle oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag des Betroffenen erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrages erforderlich ist, der im Interesse des Betroffenen von der datenverarbeitenden Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind oder
7. der Empfänger ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte bietet; die übermittelnde Stelle hat mit dem Empfänger Vereinbarungen zur Gewährleistung des Datenschutzes, insbesondere zur Zweckbindung, zu treffen.

Datenübermittlungen nach Satz 1 Nr. 7 sind dem Sächsischen Datenschutzbeauftragten innerhalb eines Monats mitzuteilen; dieser leitet die Mitteilungen an die Europäische Kommission weiter.

(4) Eine Übermittlung hat zu unterbleiben, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(5) § 16 Abs. 2 bis 4 gilt entsprechend.

Abschnitt 3
Rechte des Betroffenen

§ 18
Auskunft

(1) Dem Betroffenen ist von der datenverarbeitenden Stelle auf Antrag kostenfrei und ohne unzumutbare Verzögerung Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie die übermittelten Daten, soweit dies gespeichert oder sonst bekannt ist, und
4. die Auftragnehmer im Sinne des § 7, sofern diese Daten des Betroffenen verarbeiten.

(2) In dem Antrag soll die Art der personenbezogenen Daten näher bezeichnet werden, über die Auskunft erteilt werden soll.

(3) Sind die personenbezogenen Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, hat ihm die datenverarbeitende Stelle auf Verlangen Einsicht in die Akten zu gewähren. Werden die Akten nicht zur Person des Betroffenen geführt, wird Auskunft erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Akten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht.

(4) Die datenverarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung und Einsichtnahme nach pflichtgemäßem Ermessen; dabei dürfen berechtigte Interessen Dritter nicht beeinträchtigt werden.

(5) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die öffentliche Sicherheit gefährden oder dem Wohle des Freistaates Sachsen, eines anderen Landes oder des Bundes Nachteile bereiten würde,
2. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten notwendig ist oder
3. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung auf Grund einer Rechtsvorschrift oder wegen überwiegender berechtigter Interessen eines Dritten geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Satz 1 gilt für die Gewährung von Akteneinsicht entsprechend.

(6) Die ablehnende Entscheidung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen oder rechtlichen Gründe der mit der Ablehnung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er den Sächsischen Datenschutzbeauftragten anrufen kann. Diesem ist auf Verlangen des Betroffenen die Auskunft zu erteilen. Die Mitteilung des Sächsischen Datenschutzbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der datenverarbeitenden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Bezieht sich die Auskunft auf die Übermittlung personenbezogener Daten an

1. Staatsanwaltschaften, Polizeidienststellen und andere für die Verfolgung von Straftaten zuständige Stellen oder
2. Verfassungsschutzbehörden, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst,

darf die Auskunft nur erteilt werden, wenn der Empfänger zustimmt.

(8) Die Absätze 1 bis 7 gelten für Gerichte nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden.

§ 19
Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird bei personenbezogenen Daten in Akten festgestellt, dass sie unrichtig sind, ist dies darüber hinaus in der Akte zu vermerken. Wird die Richtigkeit personenbezogener Daten vom Betroffenen bestritten, ist dies auf geeignete Weise festzuhalten.

(2) Von der Berichtigung unrichtiger Daten sind die Empfänger übermittelter Daten zu benachrichtigen, es sei denn, die Benachrichtigung erweist sich als unmöglich oder erfordert einen unverhältnismäßig hohen Aufwand.

§ 20
Löschung

(1) Personenbezogene Daten sind zu löschen, wenn

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

(2) Personenbezogene Daten in Akten sind zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, dass die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Eine Löschung darf in den Fällen von Absatz 1 Nr. 2 und Absatz 2 erst erfolgen, nachdem die Daten dem zuständigen Archiv angeboten worden sind und dieses die Archivwürdigkeit verneint hat oder über sie nicht fristgemäß entschieden hat.

(4) Die Löschung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden,
2. sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder
3. ihr durch Rechtsvorschriften bestimmte Aufbewahrungsfristen entgegenstehen.

(5) Von einer Löschung nach Absatz 1 Nr. 1 sind die Empfänger übermittelter Daten nach Maßgabe des § 19 Abs. 2 zu verständigen.

§ 21
Sperrung

(1) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt oder
2. in den Fällen des § 20 Abs. 4 eine Löschung unterbleibt.

(2) Personenbezogene Daten in Akten sind zu sperren, wenn die datenverarbeitende Stelle im Einzelfall feststellt, dass die Daten unzulässig gespeichert sind. Sie sind ferner zu sperren, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind, eine Löschung nach § 20 Abs. 2 nicht in Betracht kommt und ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

(3) Gesperrte personenbezogene Daten sind gesondert aufzubewahren; bei automatisierten Verfahren kann die Sperrung statt dessen auch durch zusätzliche technische Maßnahmen gewährleistet werden. Lassen sich aufgrund der Art der Verarbeitung Maßnahmen nach Satz 1 nicht oder nur mit unverhältnismäßigem Aufwand durchführen, sind die Daten mit einem Sperrvermerk zu versehen.

(4) Ohne Einwilligung des Betroffenen dürfen gesperrte personenbezogene Daten nur verarbeitet werden, wenn

1. es zur Behebung einer dringenden Beweisnot in einem gerichtlichen oder Verwaltungsverfahren oder zu Aufsichts- und Kontrollzwecken unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Personenbezogene Daten, die unzulässig in Akten gespeichert sind oder deren Löschung gemäß § 20 Abs. 4 unterblieben ist, dürfen ohne Einwilligung des Betroffenen nicht mehr genutzt werden.

(5) Von einer Sperrung sind die Empfänger übermittelter Daten nach Maßgabe des § 19 Abs. 2 zu verständigen.

§ 22
Widerspruchsrecht

(1) Der Betroffene kann im Einzelfall gegenüber der datenverarbeitenden Stelle der beabsichtigten oder weiteren Verarbeitung seiner Daten widersprechen.

(2) Die Verarbeitung der Daten unterbleibt dann insoweit, als dies zur Wahrung der vom Betroffenen geltend gemachten schutzwürdigen, sich aus einer besonderen persönlichen Situation ergebenden Gründe erforderlich ist und diesen Gründen Vorrang gegenüber den Interessen der datenverarbeitenden Stelle an einer beabsichtigten oder weiteren Verarbeitung der betroffenen Daten einzuräumen ist; dies gilt nicht, wenn dem Unterbleiben der Verarbeitung eine Rechtsvorschrift entgegensteht.

(3) Die datenverarbeitende Stelle teilt dem Betroffenen das Ergebnis der Prüfung schriftlich mit.

(4) Die Absätze 1 bis 3 gelten nicht bei der Verarbeitung von Daten im Zusammenhang mit der Verfolgung von Straftaten und Ordnungswidrigkeiten.

§ 23
Schadensersatz

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist der Träger der öffentlichen Stelle dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet. Die Ersatzpflicht besteht nicht, wenn der Schaden durch ein unabwendbares Ereignis eingetreten ist.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen auch der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Sind an einer automatisierten Verarbeitung mehrere Stellen beteiligt und ist der Geschädigte nicht in der Lage, die Stelle festzustellen, die den Schaden verursacht hat, haften die Träger dieser Stellen.

(4) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(5) Auf die Verjährung, das Mitverschulden des Betroffenen und den Ausgleich unter Gesamtschuldnern sind die §§ 195 in Verbindung mit 199, §§ 254 und 426 des Bürgerlichen Gesetzbuches (BGB) entsprechend anzuwenden.

(6) Vorschriften, nach denen auch ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(7) Über Ansprüche nach den Absätzen 1 bis 5 entscheiden die ordentlichen Gerichte.

§ 24
Anrufung des Sächsischen Datenschutzbeauftragten

(1) Jeder kann sich an den Sächsischen Datenschutzbeauftragten wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine öffentliche Stelle in seinem Recht auf informationelle Selbstbestimmung verletzt worden zu sein. Dies gilt nicht, soweit eine Kontrolle durch den Sächsischen Datenschutzbeauftragten nach § 27 Abs. 1 bis 4 ausgeschlossen ist. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Satz 1 Gebrauch gemacht hat.

(2) Der Sächsische Datenschutzbeauftragte teilt dem Betroffenen und der datenverarbeitenden Stelle das Ergebnis seiner Prüfung mit. § 18 Abs. 5 und 6 Satz 4 gilt entsprechend.

Abschnitt 4
Sächsischer Datenschutzbeauftragter

§ 25
Berufung und Rechtsstellung

(1) Zur Wahrung des Rechts auf Datenschutz und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle wird beim Sächsischen Landtag der Sächsische Datenschutzbeauftragte berufen. Er wird vom Sächsischen Landtag mit der Mehrheit seiner Mitglieder auf sechs Jahre gewählt. Wählbar ist, wer die Voraussetzungen für die Berufung in das Beamtenverhältnis auf Zeit erfüllt. Der Präsident des Landtages kann die Staatsregierung um Vorschläge ersuchen.

(2) Der Präsident des Landtages ernennt den Sächsischen Datenschutzbeauftragten zum Beamten auf Zeit. Mit der Beendigung des Beamtenverhältnisses endet auch die Funktion als Sächsischer Datenschutzbeauftragter.

(3) Vor Ablauf der Amtszeit kann der Sächsische Datenschutzbeauftragte nur mit einer Mehrheit von zwei Dritteln der Mitglieder des Landtages abberufen werden. Die Vorschriften des Beamtenrechts bleiben unberührt.

(4) Der Sächsische Datenschutzbeauftragte ist in der Ausübung seines Amtes unabhängig, weisungsfrei und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Landtages, soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Für die Erfüllung seiner Aufgaben ist ihm die notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Die Besetzung der Personalstellen erfolgt im Einvernehmen mit dem Sächsischen Datenschutzbeauftragten. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit dem Sächsischen Datenschutzbeauftragten versetzt oder abgeordnet werden. Der Sächsische Datenschutzbeauftragte ist Vorgesetzter seiner Mitarbeiter. Dienstvorgesetzter und oberste Dienstbehörde des Sächsischen Datenschutzbeauftragten und seiner Mitarbeiter ist der Präsident des Landtages.

(5) Der Präsident des Landtages bestimmt im Einvernehmen mit dem Sächsischen Datenschutzbeauftragten dessen Stellvertreter.

(6) Der Sächsische Datenschutzbeauftragte und seine Mitarbeiter sind verpflichtet, über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit gegenüber jedermann zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die Verschwiegenheitspflicht besteht auch nach der Beendigung der Tätigkeit fort.

(7) Der Sächsische Datenschutzbeauftragte und seine Mitarbeiter dürfen, soweit sie zur Verschwiegenheit verpflichtet sind, nur mit Genehmigung des Präsidenten des Landtages als

Zeugen aussagen. Ihr Zeugnisverweigerungsrecht nach dem Bundesdatenschutzgesetz bleibt unberührt.

(8) Stellt der Sächsische Datenschutzbeauftragte einen strafrechtlichen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, ist er befugt, diesen bei der zuständigen Behörde zur Anzeige zu bringen. Entsprechendes gilt bei Handlungen, die als Ordnungswidrigkeit geahndet werden können.

(9) Abreden, die durch dieses Gesetz begründete Rechte und Pflichten des Sächsischen Datenschutzbeauftragten abändern, sind unwirksam.

§ 26
Anhörung des Sächsischen Datenschutzbeauftragten

Der Sächsische Datenschutzbeauftragte ist zu Entwürfen von Rechtsverordnungen und Verwaltungsvorschriften, soweit sie das Recht auf informationelle Selbstbestimmung betreffen, zu hören.

§ 27
Kontrolle durch den Sächsischen Datenschutzbeauftragten

(1) Der Sächsische Datenschutzbeauftragte kontrolliert bei den öffentlichen Stellen die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz. Seine Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

(2) Sicherheits- und Sicherheitsüberprüfungsakten unterliegen der Kontrolle durch den Sächsischen Datenschutzbeauftragten nicht, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Sächsischen Datenschutzbeauftragten widersprochen hat. Satz 1 gilt entsprechend, wenn die dort genannten Daten automatisiert verarbeitet werden. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Satz 1 Gebrauch gemacht hat.

(3) Die Kontrolle durch den Sächsischen Datenschutzbeauftragten erstreckt sich nicht auf personenbezogene Daten, die der Kontrolle durch die Kommission nach § 2 des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz im Freistaat Sachsen (SächsAG G10) vom 16. Oktober 1992 (SächsGVBl. S. 464) unterliegen, es sei denn, die Kommission ersucht den Sächsischen Datenschutzbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(4) Die Gerichte unterliegen der Kontrolle des Sächsischen Datenschutzbeauftragten nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden.

§ 28
Pflicht zur Unterstützung

(1) Die öffentlichen Stellen sind verpflichtet, den Sächsischen Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 27 insbesondere

1. Auskunft zu ihren Fragen zu geben sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, und
2. jederzeit Zutritt zu den Diensträumen zu gewähren.

(2) Der Sächsische Datenschutzbeauftragte hat den Leiter der betroffenen Stelle vor Beginn einer Kontrolle in deren Diensträumen zu informieren.

§ 29
Beanstandungen und sonstige Äußerungen

(1) Stellt der Sächsische Datenschutzbeauftragte im Rahmen seiner gesetzlichen Zuständigkeiten Verstöße gegen dieses Gesetz oder gegen andere Vorschriften über den Datenschutz fest, beanstandet er dies schriftlich

1. bei den öffentlichen Stellen des Freistaates Sachsen gegenüber der zuständigen obersten Landesbehörde,
2. bei den Gemeinden, Landkreisen und sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts gegenüber dem vertretungsberechtigten Organ sowie
3. bei Beliehenen gegenüber dem vertretungsberechtigten Organ oder, soweit es sich um eine natürliche Person handelt, gegenüber dieser selbst

nach deren Anhörung und fordert zur Stellungnahme und Behebung der Verstöße innerhalb einer von ihm zu bestimmenden angemessenen Frist auf. In den Fällen des Satzes 1 Nr. 2 und 3 unterrichtet der Sächsische Datenschutzbeauftragte gleichzeitig die zuständige Aufsichtsbehörde. In seiner Beanstandung setzt sich der Sächsische Datenschutzbeauftragte inhaltlich mit dem Vorbringen der öffentlichen Stelle auseinander.

(2) Der Sächsische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Sächsischen Datenschutzbeauftragten getroffen worden oder beabsichtigt sind. Die in Absatz 1 Satz 1 Nr. 2 und 3 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Sächsischen Datenschutzbeauftragten zu.

§ 30
Tätigkeitsbericht und weitere Aufgaben

(1) Der Sächsische Datenschutzbeauftragte erstattet dem Landtag alle zwei Jahre jeweils zum 31. März einen Bericht über seine Tätigkeit; er veröffentlicht diesen Bericht.

(2) Der Sächsische Datenschutzbeauftragte kann sich im Rahmen seiner gesetzlichen Zuständigkeiten jederzeit an den Landtag wenden.

(3) Der Sächsische Datenschutzbeauftragte hat auf Anforderung des Landtages oder der Staatsregierung Gutachten und besondere Berichte zu Fragen des Datenschutzes zu erstatten. Auf Beschluss des Landtages oder auf Ersuchen der Staatsregierung geht der Sächsische Datenschutzbeauftragte Hinweisen auf Angelegenheiten nach, die den Datenschutz in dem seiner Kontrolle unterliegenden Bereich betreffen.

(4) Der Sächsische Datenschutzbeauftragte kann die Staatsregierung und einzelne Staatsministerien sowie andere öffentliche Stellen in Fragen des Datenschutzes beraten und ihnen Empfehlungen zur Verbesserung des Datenschutzes geben. Soll die Empfehlung einem anderen zugänglich gemacht werden, gilt § 29 Abs. 4 entsprechend.

§ 31
Datenschutzregister

(1) Der Sächsische Datenschutzbeauftragte führt ein Register der ihm nach § 10 Abs. 3 zugeleiteten Verzeichnisse (Datenschutzregister).

(2) Der Sächsische Datenschutzbeauftragte erteilt auf Antrag im Einzelfall jedermann Auskunft über die Angaben nach § 10 Abs. 1 Satz 2 Nr. 1 bis 7. Hiervon sind ausgenommen die Verzeichnisse der in § 18 Abs. 7 genannten Stellen. § 18 bleibt unberührt.

Abschnitt 5
Sonstige Vorschriften

§ 32
Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen und Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und danach schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen ferngesteuerte Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmess- oder Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird. Der Betroffene kann seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass der Betroffene nach Absatz 1 Satz 1 oder 2 einwilligt. Verweigert oder widerruft er seine Einwilligung, dürfen ihm keine Nachteile entstehen, die über die nachweisbaren Mehrkosten einer anderen Art der Datenerhebung hinausgehen.

§ 33
Videoüberwachung und Videoaufzeichnung

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit dies zur Aufgabenerfüllung, insbesondere zur Gewährleistung der öffentlichen Sicherheit und Ordnung, oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Interessen Betroffener nicht überwiegen.

(2) Die Tatsache der Videoüberwachung und die verantwortliche Stelle sind, soweit nicht offenkundig, durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung von nach Absatz 1 erhobenen Daten (Videoaufzeichnung) und deren weitere Verarbeitung ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von Straftaten und Ordnungswidrigkeiten erforderlich ist.

(4) Das nach Absatz 1 gewonnene Bildmaterial und daraus gefertigte Unterlagen sind spätestens nach zwei Monaten zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von Rechtsansprüchen oder wegen entgegenstehender schutzwürdiger Interessen Betroffener, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich sind. § 20 Abs. 3 bleibt unberührt.

§ 34
Automatisierte Einzelentscheidungen

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder diesen erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung zum Zweck der Bewertung einzelner Persönlichkeitsmerkmale gestützt werden.

(2) Absatz 1 gilt nicht, soweit

1. eine solche Verarbeitung durch Rechtsvorschrift vorgeschrieben oder zugelassen ist,
2. mit der Entscheidung dem Begehren des Betroffenen stattgegeben wird oder
3. dem Betroffenen die Entscheidung unter Hinweis darauf, dass es sich um eine automatisierte Einzelentscheidung handelt, mitgeteilt und ihm Gelegenheit zur Stellungnahme gegeben wird; die öffentliche Stelle hat die Entscheidung nach Eingang der Stellungnahme erneut zu prüfen.

(3) Das Recht des Betroffenen auf Auskunft nach § 18 erstreckt sich auch auf den strukturierten Ablauf der automatisierten Verarbeitung seiner personenbezogenen Daten und die dabei herangezogenen Entscheidungskriterien.

§ 35
Mobile personenbezogene Datenverarbeitungsmedien

(1) Mobile personenbezogene Datenverarbeitungsmedien zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten der Betroffenen automatisiert austauschen können, dürfen nur eingesetzt werden, soweit dies eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung zulässt oder der Betroffene eingewilligt hat.

(2) Für den Betroffenen muss erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungsmedium oder durch dieses veranlasst stattfinden,
2. welche personenbezogenen Daten des Betroffenen verarbeitet werden und
3. welcher Verarbeitungsvorgang im Einzelnen abläuft oder angestoßen wird.

(3) Der Betroffene ist bei der Ausgabe des mobilen Datenverarbeitungsmediums über die ihm nach den §§ 18 bis 22 zustehenden Rechte und über die bei Verlust oder Zerstörung des mobilen Datenverarbeitungsmediums zu treffenden Maßnahmen aufzuklären.

§ 36
Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung

(1) Personenbezogene Daten einschließlich solcher nach § 4 Abs. 2 dürfen verarbeitet werden, soweit dies für die Durchführung der wissenschaftlichen Forschung erforderlich ist, insbesondere der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, und wenn das öffentliche, insbesondere das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Unterbleiben der Verarbeitung überwiegt.

(2) Soweit es der Forschungszweck erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, getrennt zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck dies zulässt.

(3) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, soweit

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(5) Soweit die Vorschriften dieses Gesetzes auf den Empfänger der Daten keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 1 bis 4 einzuhalten.

(6) Soweit Forschung betreibende Stellen personenbezogene Daten zum Zweck der Durchführung wissenschaftlicher Forschung verarbeiten, haben diese einen Datenschutzbeauftragten gemäß § 11 zu bestellen. § 11 Abs. 3 Satz 2 Nr. 4 findet keine Anwendung. Bei der Mitteilung nach § 11 Abs. 3 Satz 2 Nr. 5 darf die Beschreibung der Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden, auf die Angabe „Forschungsvorhaben“ beschränkt werden.

§ 37
Schutz von Beschäftigtendaten im öffentlichen Dienst

(1) Öffentliche Stellen dürfen Daten von Bewerbern oder Beschäftigten nur verarbeiten, soweit 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 ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Dies gilt auch für Daten Dritter, deren Verarbeitung für die in Satz 1 genannten Zwecke erforderlich ist. Die Verarbeitung der in § 4 Abs. 2 genannten Daten ist nur zulässig, wenn dies zur Erreichung der in Satz 1 genannten Zwecke zwingend erforderlich ist.

(2) Eine Veröffentlichung der Daten von Beschäftigten ist nur zulässig, wenn

1. der Betroffene eingewilligt hat oder
2. diese für die Information der Allgemeinheit oder der anderen Beschäftigten erforderlich ist und ihr keine schutzwürdigen Interessen des Betroffenen entgegenstehen.

(3) Abweichend von § 16 ist eine Übermittlung der Daten von Beschäftigten an natürliche Personen oder andere nicht-öffentliche Stellen nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht,
2. der Betroffene eingewilligt hat oder
3. die Voraussetzungen für eine Veröffentlichung nach Absatz 2 vorliegen.

Für die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber gilt nur Satz 1 Nr. 1 und 2.

(4) Das Auskunftsrecht nach § 18 umfasst auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 5 Nr. 3 findet keine Anwendung.

(5) Daten, die vor Beginn eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, dass durch die

Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Der Betroffene ist hiervon zu verständigen.

(6) Daten von Beschäftigten, die zur Verhaltens- oder Leistungskontrolle erhoben werden, dürfen nur zu diesem Zweck verarbeitet werden.

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

§ 38
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
   a) verarbeitet,
   b) zum Abruf bereithält oder
   c) für sich oder einen anderen abruft oder auf andere Weise verschafft,
2. die Übermittlung von personenbezogenen Daten, die durch dieses Gesetz geschützt werden und nicht offenkundig sind, durch unrichtige Angaben erschleicht,
3. nach einer Verpflichtung gemäß § 6 Abs. 2 das Datengeheimnis gemäß § 6 Abs. 1 Satz 1 oder 2 verletzt, wenn die Verletzung nicht mit Strafe bedroht ist,
4. entgegen § 11 Abs. 2 Satz 3 den Datenschutzbeauftragten einer öffentlichen Stelle wegen der Erfüllung seiner Aufgaben benachteiligt,
5. als Datenschutzbeauftragter einer öffentlichen Stelle seine Verschwiegenheitspflicht nach § 11 Abs. 4 Satz 1 verletzt, wenn die Verletzung nicht mit Strafe bedroht ist,
6. personenbezogene Daten ohne die nach § 14 Abs. 3 Satz 3 oder nach § 16 Abs. 4 Satz 3 erforderliche Einwilligung oder entgegen § 36 Abs. 3 für einen anderen Zweck verarbeitet,
7. eine Auskunft nach § 18 Abs. 1 unrichtig oder unvollständig erteilt,
8. entgegen § 24 Abs. 1 Satz 3 einen anderen benachteiligt oder maßregelt, weil er von seinem Recht auf Anrufung des Sächsischen Datenschutzbeauftragten Gebrauch gemacht hat,
9. entgegen § 27 Abs. 2 Satz 3 einen anderen benachteiligt oder maßregelt, weil er von seinem Recht, die Einwilligung zu verweigern, Gebrauch gemacht hat,
10. bei der Datenverarbeitung im Auftrag als Auftragnehmer gegen eine Weisung des Auftraggebers gemäß § 7 Abs. 2 Satz 4 und 5 verstößt,
11. entgegen § 16 Abs. 5 eine vollziehbare Auflage oder eine Vereinbarung nicht, nicht rechtzeitig oder nicht vollständig erfüllt oder
12. entgegen § 36 Abs. 2 die dort bezeichneten Merkmale nicht getrennt speichert.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 25 000 EUR geahndet werden.

(3) Verwaltungsbehörden im Sinne von § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) in der Fassung der Bekanntmachung vom 19. Februar 1987

(BGBl. I S. 602), zuletzt geändert durch Artikel 2 Abs. 8 des Gesetzes vom 19. April 2001 (BGBl. I S. 623, 633), in der jeweils geltenden Fassung, sind die Regierungspräsidien.

§ 39
Straftaten

Wer eine der in § 38 Abs. 1 Nr. 1 bis 9 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

§ 40
Übergangsregelungen

(1) Bei einer Änderung automatisierter Verarbeitungsverfahren sind diese vor der erneuten Inbetriebnahme an die Vorschriften dieses Gesetzes anzupassen. Unabhängig von Satz 1 hat die Anpassung automatisierter Verarbeitungsverfahren binnen drei Jahren nach In-Kraft-Treten dieses Gesetzes zu erfolgen.

(2) Personenbezogene Daten im Sinne von § 4 Abs. 2, die bisher in zulässiger Art und Weise verarbeitet wurden, deren weitere Verarbeitung aber nach In-Kraft-Treten dieses Gesetzes nicht mehr zulässig ist, sind binnen zwei Jahren nach In-Kraft-Treten dieses Gesetzes zu löschen.

§ 41
Einschränkung eines Grundrechts

Das Grundrecht auf informationelle Selbstbestimmung nach Artikel 33 der Verfassung des Freistaates Sachsen wird durch dieses Gesetz eingeschränkt.

§ 42
In-Kraft-Treten und Außer-Kraft-Treten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft. Gleichzeitig tritt das Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) vom 11. Dezember 1991 (SächsGVBl. S. 401), geändert durch Artikel 2 des Gesetzes vom 7. April 1997 (SächsGVBl. S. 350, 351), außer Kraft.