

Gesetz
zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen
(Sächsisches Datenschutzgesetz – SächsDSG)

Vom 11. Dezember 1991

Der Sächsische Landtag hat am 21. November 1991 das folgende Gesetz beschlossen:

Inhaltsübersicht

Erster Abschnitt: Allgemeine Vorschriften

- § 1 Zweck des Gesetzes
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen
- § 4 Zulässigkeit der Datenverarbeitung
- § 5 Rechte des Betroffenen
- § 6 Datengeheimnis
- § 7 Datenverarbeitung im Auftrag
- § 8 Automatisiertes Abrufverfahren
- § 9 Maßnahmen zur Gewährleistung des Datenschutzes
- § 10 Dateien- und Geräteverzeichnis

Zweiter Abschnitt: Rechtsgrundlagen der Datenverarbeitung

- § 11 Erhebung
- § 12 Speicherung, Veränderung und Nutzung
- § 13 Übermittlung an öffentliche Stellen
- § 14 Übermittlung an öffentlich-rechtliche Religionsgesellschaften
- § 15 Übermittlung an nicht-öffentliche Stellen
- § 16 Übermittlung an Stellen im Ausland

Dritter Abschnitt: Rechte des Betroffenen

- § 17 Auskunft
- § 18 Berichtigung
- § 19 Löschung
- § 20 Sperrung
- § 21 Schadensersatz
- § 22 Anrufung des Datenschutzbeauftragten

Vierter Abschnitt: Sächsischer Datenschutzbeauftragter

- § 23 Berufung und Rechtsstellung
- § 24 Kontrolle durch den Datenschutzbeauftragten
- § 25 Pflicht zur Unterstützung
- § 26 Beanstandungen
- § 27 Jahresbericht und weitere Aufgaben
- § 28 Mitteilungen aus dem Dateien- und Geräteverzeichnis

Fünfter Abschnitt: Sonstige Vorschriften

- § 29 Fernmessen und Fernwirken
- § 30 Verarbeitung personenbezogener Daten durch Forschungseinrichtungen
- § 31 Datenschutz im öffentlichen Dienst
- § 32 Ordnungswidrigkeiten
- § 33 Straftaten
- § 34 Übergangsregelung
- § 35 Altdatenbestände
- § 36 Inkrafttreten

Erster Abschnitt
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 in seinem Persönlichkeitsrecht, insbesondere 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) Natürliche und juristische Personen sowie Vereinigungen des privaten Rechts gelten als öffentliche Stellen im Sinne dieses Gesetzes, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Dies gilt nicht, sofern sie als öffentliche Stellen des Bundes im Sinne des § 2 Abs. 3 und 4 des Bundesdatenschutzgesetzes gelten.

(3) Soweit öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, gelten für sie und ihre Vereinigungen die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts.

(4) Soweit besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes den Schutz personenbezogener Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor. Die Kontrollbefugnisse des Datenschutzbeauftragten bleiben unberührt.

§ 3

Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (Betroffener).

(2) Verarbeiten ist das Erheben, Speichern, Verändern, 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 einer bestimmten oder bestimmbarer 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) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruf,
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.

(5) Eine Datei ist

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).

(6) Eine Akte ist jeder sonstige, amtlichen oder dienstlichen Zwecken dienende Träger personenbezogener Daten; dazu zählen auch Bild- und Tonträger, soweit sie nicht Dateien im Sinne des Absatzes 5 sind.

§ 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) Wer die Einwilligung des Betroffenen einholt, hat ihn zuvor auf den Zweck der Datenverarbeitung, die Empfänger einer vorgesehenen Datenübermittlung sowie auf sein Recht zur Verweigerung der Einwilligung und die etwaigen Folgen der Verweigerung hinzuweisen. Rechtsnachteile dürfen dem Betroffenen durch die Verweigerung der Einwilligung nicht entstehen.

(3) 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

Rechte des Betroffenen

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

1. Auskunft über die zu seiner Person gespeicherten Daten (§ 17),
2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§§ 18 bis 20),
3. Schadensersatz (§ 21),
4. Anrufung des Datenschutzbeauftragten (§ 22).

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

(3) Sind die Daten des Betroffenen in einer Datei gespeichert, an der mehrere Stellen beteiligt sind, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die zuständige Stelle

weiterzuleiten. Der Betroffene ist über die Weiterleitung und die zuständige Stelle zu unterrichten.

§ 6 Datengeheimnis

(1) Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

(2) Die in Absatz 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

(1) Bei der Datenverarbeitung im Auftrag ist auch der Auftraggeber für die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz 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 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.

§ 8 Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, darf nur eingerichtet werden, soweit ein Gesetz dies ausdrücklich zuläßt.

(2) Die Einrichtung eines automatisierten Verfahrens, das den Abruf personenbezogener Daten nur innerhalb einer öffentlichen Stelle ermöglicht, ist zulässig, wenn dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der öffentlichen Stelle angemessen ist und eine mindestens stichprobenweise Abrufkontrolle gewährleistet ist. Vor Aufnahme des Abrufverfahrens sind schriftlich festzulegen:

1. der Anlaß und der Zweck des Abrufverfahrens,
2. die Datenempfänger,
3. die abrufbaren Daten und
4. die Maßnahmen zur Gewährleistung des Datenschutzes (§ 9).

(3) Vor der Einrichtung eines Abrufverfahrens im Sinne der Absätze 1 oder 2 ist der Datenschutzbeauftragte zu unterrichten.

(4) Die Absätze 1 bis 3 gelten nicht für den Abruf aus Datenbeständen, die der Allgemeinheit zur Benutzung offenstehen 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 verarbeitet, sind nach dem jeweiligen Stand der Technik die Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß
 - a) überprüft und festgestellt werden kann, an wen welche Daten durch Einrichtungen zur Datenübertragung übermittelt werden können,
 - b) mindestens stichprobenweise überprüft und festgestellt werden kann, wann und an wen welche personenbezogenen Daten übermittelt worden sind (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

9. zu gewährleisten, daß bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
 10. die innere Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).
- (3) Die Staatsregierung wird ermächtigt, im Einvernehmen mit dem Datenschutzbeauftragten durch Rechtsverordnung die in Absatz 1 und 2 genannten Anforderungen und Maßnahmen nach dem jeweiligen Stand der Technik näher zu bestimmen und fortzuschreiben.
- (4) Werden personenbezogene Daten in nicht-automatisierten Dateien oder 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 Dateien- und Geräteverzeichnis

(1) Jede öffentliche Stelle führt ein Verzeichnis ihrer Dateien und der eingesetzten Datenverarbeitungsanlagen. In dem Verzeichnis sind schriftlich festzuhalten:

1. die Bezeichnung der Datei und ihre Zweckbestimmung,
2. die Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden und die Rechtsgrundlage der Verarbeitung,
3. die Art der gespeicherten Daten,
4. der Kreis der Betroffenen,
5. die Art der regelmäßig zu übermittelnden Daten und deren Empfänger sowie die Art und Herkunft der regelmäßig zu empfangenden Daten,
6. die Fristen für die Prüfung der Sperrung und Löschung der Daten sowie für die Sperrung und Löschung,
7. die zugriffsberechtigten Personen oder Personengruppen,
8. die personellen, technischen und organisatorischen Maßnahmen gemäß § 9,
9. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie die Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung,
10. Typ, Art, Hersteller und Gerätenummern der bei der automatisierten Datenverarbeitung eingesetzten Geräte, das verwendete Betriebssystem sowie die Möglichkeiten zur Datenfernverarbeitung und Datenübertragung.

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

Zweiter Abschnitt Rechtsgrundlagen der Datenverarbeitung

§ 11 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 ist ihm 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, so 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 ein Gesetz oder eine Rechtsverordnung dies vorsieht oder zwingend voraussetzt.

(4) Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn

1. ein Gesetz oder eine Rechtsverordnung 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 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 Bereichs erhoben, so 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.

§ 12

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, so sind die Zwecke maßgebend, für die die Daten erstmals 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 § 11 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** oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des **Jugendgerichtsgesetzes** oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist oder
 4. es zur Durchführung wissenschaftlicher Forschung erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Unterbleiben der Zweckänderung erheblich überwiegt; dies gilt nicht, wenn der Zweck der Forschung durch die Verwendung anonymisierter Daten erreicht werden kann.
- (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 Zweck 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 Absatz 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, so 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.

§ 13

Übermittlung an öffentliche Stellen

- (1) Die Übermittlung personenbezogener Daten an öffentliche Stellen im Sinne dieses Gesetzes sowie an öffentliche Stellen anderer Länder und des Bundes ist zulässig, wenn sie
1. zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und
 2. für Zwecke erfolgt, für die eine Nutzung nach § 12 Abs. 1 bis 4 zulässig wäre.
- (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 § 12 Abs. 2 zulässig. Unterliegen die übermittelten Daten einem Berufs- oder besonderen Amtsgeheimnis, so 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 § 12 Abs. 5 entsprechend.

§ 14

Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Für die Übermittlung personenbezogener Daten an öffentlich-rechtliche Religionsgesellschaften gilt § 13 entsprechend, sofern für den Empfänger ausreichende Datenschutzregelungen gelten. Die Feststellung hierüber trifft das Staatsministerium für Kultus im Einvernehmen mit dem Datenschutzbeauftragten.

§ 15

Übermittlung an nicht-öffentliche Stellen

- (1) Die Übermittlung personenbezogener Daten an andere als die in §§ 13, 14 und 16 genannten Personen oder Stellen ist zulässig, wenn
1. sie zur Erfüllung der Aufgaben der übermittelnden Stellen erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach § 12 Abs. 1 bis 4 zulässig wäre, 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) 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.

§ 16 Übermittlung an Stellen im Ausland

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb der Bundesrepublik Deutschland sowie an über- und zwischenstaatliche Stellen ist zulässig, soweit sie in einer Rechtsvorschrift oder einem Rechtsakt der Europäischen Gemeinschaften geregelt ist. Im übrigen ist die Übermittlung unter den Voraussetzungen des § 15 Abs. 1 zulässig, soweit keine Anhaltspunkte dafür vorliegen, daß ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(3) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur für den Zweck verarbeitet werden dürfen, zu dessen Erfüllung sie ihm übermittelt wurden.

(4) § 15 Abs. 2 und 3 gilt entsprechend.

Dritter Abschnitt Rechte des Betroffenen

§ 17 Auskunft

(1) Dem Betroffenen ist von der speichernden Stelle auf Antrag kostenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck der Speicherung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie die übermittelten Daten, soweit dies gespeichert oder sonst bekannt ist.

(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, so hat ihm die speichernde Stelle auf Verlangen Einsicht in die Akten zu gewähren. Werden die Akten nicht zur Person des Betroffenen geführt, so 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. Satz 2 findet auf personenbezogene Daten in nichtautomatisierten Dateien, die nicht zur Übermittlung an Dritte bestimmt sind, entsprechende Anwendung.

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

(5) Die Auskunftserteilung unterbleibt, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen überwiegender Geheimhaltungsinteressen der speichernden Stelle oder eines Dritten geheimgehalten 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 Datenschutzbeauftragten anrufen kann. Diesem ist auf Verlangen des Betroffenen die Auskunft zu erteilen. Die Mitteilung des Datenschutzbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden 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,

so darf die Auskunft nur erteilt werden, wenn der Empfänger erklärt, daß die Voraussetzungen für eine ablehnende Entscheidung nach Absatz 5 nicht vorliegen.

§ 18 Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird bei personenbezogenen Daten in Akten festgestellt, daß sie unrichtig sind, oder wird ihre Richtigkeit vom Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Von der Berichtigung unrichtiger Daten ist der Empfänger übermittelter Daten zu benachrichtigen, soweit dies zur Wahrung schutzwürdiger Interessen des Betroffenen oder zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich erscheint. Sind die unrichtigen Daten nicht im Rahmen regelmäßiger Datenübermittlung übermittelt worden, erfolgt eine Benachrichtigung nach Satz 1 nur, soweit Angaben über die Empfänger und die übermittelten Daten gespeichert oder sonst bekannt sind.

§ 19
Löschung

- (1) Personenbezogene Daten in Dateien 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) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem staatlichen Archiv zur Übernahme anzubieten, darf eine Löschung erst erfolgen, wenn das zuständige staatliche Archiv die Übernahme abgelehnt 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, oder
 2. sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
- (5) Von einer Löschung nach Absatz 1 Nr. 1 sind die Empfänger übermittelter Daten nach Maßgabe des § 18 Abs. 2 zu verständigen.

§ 20
Sperrung

- (1) Personenbezogene Daten in Dateien 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 § 19 Abs. 4 eine Löschung unterbleibt.
- (2) Personenbezogene Daten in Akten sind zu sperren, wenn die speichernde 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 § 19 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 unverhältnismäßig hohem 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- oder 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 § 19 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 § 18 Abs. 2 zu verständigen.

§ 21
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 automatisierte Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.
- (2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.
- (3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 250 000 DM begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 250 000 DM übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.
- (4) Sind bei einer Datei mehrere Stellen speicherungs berechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.
- (5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.
- (6) Auf das Mitverschulden des Betroffenen, den Ausgleich unter Gesamtschuldnern und die Verjährung sind die §§ 254, 426 und 852 des [Bürgerlichen Gesetzbuches](#) entsprechend anzuwenden.
- (7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang haftet oder nach denen auch ein anderer für den Schaden verantwortlich ist, bleiben unberührt.
- (8) Über Ansprüche nach den Absätzen 1 bis 6 entscheiden die ordentlichen Gerichte.

§ 22
Anrufung des Datenschutzbeauftragten

Jeder kann sich an den Datenschutzbeauftragten wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine öffentliche Stelle in seinen Rechten verletzt worden zu sein. Für die Verarbeitung personenbezogener Daten durch die Gerichte gilt dies nur, soweit sie der Kontrolle nach § 24 Abs. 2 unterliegen. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Satz 1

Gebrauch gemacht hat.

Vierter Abschnitt Sächsischer Datenschutzbeauftragter

§ 23 Berufung und Rechtsstellung

(1) Zum Schutz des Rechts auf informationelle Selbstbestimmung und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle wird beim Sächsischen Landtag der Sächsische Datenschutzbeauftragte (Datenschutzbeauftragter) berufen. Er wird vom Sächsischen Landtag mit der Mehrheit seiner Mitglieder auf sechs Jahre gewählt. Der Präsident des Landtages kann die Staatsregierung um Vorschläge ersuchen.

(2) Der Präsident des Landtages ernennt den Datenschutzbeauftragten zum Beamten auf Zeit.

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

(4) Der 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 Datenschutzbeauftragten. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit dem Datenschutzbeauftragten versetzt oder abgeordnet werden. Der Datenschutzbeauftragte ist Vorgesetzter seiner Mitarbeiter.

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

(6) Der Datenschutzbeauftragte und seine Mitarbeiter sind verpflichtet, über die ihnen bei ihrer Tätigkeit bekanntgewordenen personenbezogenen Daten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr und für allgemein zugängliche Daten. Die Verschwiegenheitspflicht besteht auch nach der Beendigung der Tätigkeit fort.

(7) Der Datenschutzbeauftragte und seine Mitarbeiter dürfen, soweit sie zur Verschwiegenheit verpflichtet sind, nur mit Genehmigung des Präsidenten des Landtages als Zeugen aussagen. Ihr Zeugnisverweigerungsrecht nach § 12 Abs. 3 in Verbindung mit § 23 Abs. 4 des Bundesdatenschutzgesetzes bleibt unberührt.

§ 24 Kontrolle durch den Datenschutzbeauftragten

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

§ 25 Pflicht zur Unterstützung

Die öffentlichen Stellen sind verpflichtet, den Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 24 insbesondere

1. Auskunft zu ihren Fragen 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,
2. jederzeit Zutritt zu den Diensträumen zu gewähren.

§ 26 Beanstandungen

(1) Stellt der Datenschutzbeauftragte Verstöße gegen dieses Gesetz oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

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 sowie bei öffentlichen Stellen im Sinne des § 2 Abs. 2 gegenüber dem vertretungsberechtigten Organ

nach deren Anhörung und fordert zur Mängelbeseitigung innerhalb einer von ihm zu bestimmenden angemessenen Frist auf. In den Fällen des Satzes 1 Nr. 2 unterrichtet der Datenschutzbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der 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 Datenschutzbeauftragten getroffen worden oder beabsichtigt sind. Die in Absatz 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Datenschutzbeauftragten zu.

§ 27 Jahresbericht und weitere Aufgaben

- (1) Der Datenschutzbeauftragte erstattet dem Landtag jährlich zum 31. März einen Tätigkeitsbericht für das abgelaufene Jahr.
- (2) Der Datenschutzbeauftragte kann sich jederzeit an den Landtag wenden.
- (3) Der Datenschutzbeauftragte hat auf Anforderung des Landtages oder der Staatsregierung Gutachten zu erstellen und besondere Berichte zu erstatten. Auf Ersuchen des Landtages oder der Staatsregierung geht der Datenschutzbeauftragte Hinweisen auf Angelegenheiten nach, die den Datenschutz in dem seiner Kontrolle unterliegenden Bereich betreffen.
- (4) Der Datenschutzbeauftragte kann der Staatsregierung und einzelnen Staatsministerien sowie anderen öffentlichen Stellen Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten.

§ 28

Mitteilungen aus dem Dateien- und Geräteverzeichnis

- (1) Die öffentlichen Stellen im Sinne des § 2 sind verpflichtet, die nach § 10 zu führenden Dateien- und Geräteverzeichnisse dem Datenschutzbeauftragten auf dessen Anforderung zuzuleiten.
- (2) Der Datenschutzbeauftragte erteilt auf Antrag im Einzelfall jedermann Auskunft über die Angaben nach § 10 Abs. 1 Nr. 1bis 6. Hiervon sind ausgenommen die Verzeichnisse der in § 17 Abs. 7 genannten Stellen. § 17 bleibt unberührt.

Fünfter Abschnitt Sonstige Vorschriften

§ 29

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, so dürfen ihm keine Nachteile entstehen, die über die nachweisbaren Mehrkosten einer anderen Art der Datenerhebung hinausgehen.

§ 30

Verarbeitung personenbezogener Daten durch Forschungseinrichtungen

- (1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.
- (2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten und die Vorschriften der Absätze 3 und 4 einzuhalten.
- (3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.
- (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) Bei der Mitteilung nach § 28 Abs. 2 darf die Beschreibung der Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden, auf die Angabe „Forschungsvorhaben“ beschränkt werden.

§ 31

Datenschutz im öffentlichen Dienst

- (1) Öffentliche Stellen dürfen Daten von Bewerbern oder Beschäftigten nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung 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, denen Rechte aus dem Dienst- und Arbeitsverhältnis zustehen.¹
- (2) Abweichend von § 15 ist eine Übermittlung der Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereiches nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen zulässig. Dies gilt auch für Datenübermittlungen an einen künftigen Dienstherrn oder Arbeitgeber des Betroffenen. Ausgenommen sind die im Dienstverkehr zwingend erforderlichen Auskünfte.
- (3) Das Auskunftsrecht nach § 17 umfaßt auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 17 Abs. 5 findet keine Anwendung.
- (4) 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.

(5) Daten, die zur Verhaltens- oder Leistungskontrolle erhoben werden, dürfen nur zu diesem Zweck genutzt werden.

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

(7) Eine automatisierte Verarbeitung von Daten der Beschäftigten darf nur im Benehmen mit dem Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden. Die Stellungnahme des Datenschutzbeauftragten ist den zuständigen Personalvertretungen im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens zuzuleiten.

§ 32 Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
 - a) speichert, verändert oder übermittelt,
 - b) zum Abruf mittels automatisierten Verfahrens bereithält oder
 - c) abrufen oder sich oder einem anderen aus Dateien verschafft,
2. die Übermittlung von personenbezogenen Daten, die durch dieses Gesetz geschützt werden und nicht offenkundig sind, durch unrichtige Angaben erschleicht,
3. personenbezogene Daten ohne die nach § 13 Abs. 3 Satz 3 oder nach § 15 Abs. 4 Satz 3 erforderliche Einwilligung oder entgegen § 30 Abs. 1 für einen anderen Zweck nutzt,
4. entgegen § 30 Abs. 3 Satz 3 die in § 30 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt oder
5. entgegen § 15 Abs. 5 eine vollziehbare Auflage nicht, nicht rechtzeitig oder nicht vollständig erfüllt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 DM geahndet werden.

(3) Verwaltungsbehörden im Sinne von § 36 Abs. 1 Nr. 1 des [Gesetzes über Ordnungswidrigkeiten](#) sind die Regierungspräsidien.

§ 33 Straftaten

Wer eine der in § 32 Abs. 1 Nr. 1 bis 4 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.

§ 34 Übergangsregelung

(1) Bis zum 31. März 1992 sind vorzunehmen

1. die Verpflichtung nach § 6 Abs. 2 für Personen, die bei Inkrafttreten dieses Gesetzes mit der Datenverarbeitung öffentlicher Stellen beschäftigt sind,
2. die Unterrichtung nach § 8 Abs. 3 für die bei Inkrafttreten dieses Gesetzes eingerichteten Abrufverfahren,
3. die Erstellung der Verzeichnisse nach § 10 für die bei Inkrafttreten dieses Gesetzes eingesetzten Dateien und Datenverarbeitungsanlagen.

(2) Im übrigen sind die bei Inkrafttreten dieses Gesetzes vorhandenen Dateien und automatisierten Verfahren bis spätestens 31. Dezember 1992 den Vorschriften dieses Gesetzes anzupassen.

§ 35 Altdateienbestände

(1) Wer die tatsächliche Gewalt über personenbezogene Daten in Akten oder Dateien innehat, die von ehemaligen staatlichen oder wirtschaftsleitenden Organen, Kombinat, Betrieben oder Einrichtungen sowie gesellschaftlichen Organisationen der Deutschen Demokratischen Republik auf dem Gebiet des Freistaates Sachsen für Zwecke der öffentlichen Verwaltung erhoben oder in anderer Weise verarbeitet wurden, gilt als öffentliche Stelle im Sinne dieses Gesetzes.

(2) Die in Absatz 1 genannten Personen und Stellen sind verpflichtet, bis zum 31. März 1992 über die in ihrer tatsächlichen Gewalt befindlichen Akten oder Dateien ein Verzeichnis in sinngemäßer Anwendung des § 10 dem Datenschutzbeauftragten zur Auswertung zuzuleiten und darzulegen, welche Akten, Dateien und Geräte zur rechtmäßigen Aufgabenerfüllung noch erforderlich sind. Sie sind ferner verpflichtet, die in ihrer tatsächlichen Gewalt befindlichen Akten oder Dateien unverzüglich unter Verschluss zu nehmen.

(3) Jedermann ist verpflichtet, sich an den Datenschutzbeauftragten zu wenden und über nicht mehr vorhandene Akten und Dateien die in § 10 vorgeschriebenen Angaben zu machen, soweit dies den Umständen und seiner Kenntnis nach noch möglich ist.

(4) Die in Absatz 1 genannten Personen und Stellen haben Akten und Dateien im Sinne des Absatzes 1 sowie die zu ihrer Ordnung, Auffindung oder Auswertung dienenden Materialien und Träger sowie sämtliches Zubehör dem Sächsischen Staatsministerium des Innern oder einer von diesem genannten Behörde im Original und mit sämtlichen Ausfertigungen auf Verlangen zur Einsicht vorzulegen und zu übergeben. Kopien dürfen weder angefertigt noch behalten werden. §§ 24 und 25 bleiben unberührt.

(5) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. Datenbestände im Sinne des Absatzes 1 oder 3 verheimlicht,

2. die Vorlage eines Verzeichnisses nach Absatz 2 unterläßt,
3. Akten oder Dateien entgegen Absatz 4 nicht vorlegt, nicht übergibt oder Kopien anfertigt oder zurückbehält.

§ 36 Inkrafttreten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft. Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Dresden, den 11. Dezember 1991

**Der Ministerpräsident
Prof. Dr. Kurt Biedenkopf**

**Der Staatsminister des Innern
Heinz Eggert**

1 § 31 Absatz1 geändert durch [Artikel 2 des Gesetzes vom 7. April 1997](#) (SächsGVBl. S. 350, 351)