DER HESSISCHE DATENSCHUTZBEAUFTRAGTE

Datenschutz in Schulen

Datenschutz in Schulen

Überblick und Materialien
zur Durchführung des
Datenschutzes in Schulen

Inhaltsverzeichnis

Vorwort

Am 1. August 1993 trat das **Hessische Schulgesetz vom 17. Juni 1992** (GVBl. I S. 233) in Kraft. Der Gesetzgeber hatte damit nicht nur das Schulrecht völlig neu geordnet, sondern auch die Verarbeitung personenbezogener Daten in Schulen an eine Reihe von Bedingungen geknüpft. Inzwischen ist das Schulgesetz mehrfach geändert worden. Die Änderung vom 29. November 2004 (GVBl. I S. 330) betraf auch datenschutzrechtliche Bestimmungen. Die Fassung vom 14. Juni 2005 (GVBl. I S. 442) wurde zuletzt geändert durch Gesetz vom 14. Juli 2009 (GVBl. I S. 265). Ergänzt werden diese Vorschriften durch die vom Hessischen Kultusminister erlassene **Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. 3/2009 S. 131).**

Diese Broschüre soll Schülerinnen und Schülern, Erziehungsberechtigten, Lehrerinnen, Lehrern und Schulleitungen einen Überblick über das aktuelle Datenschutzrecht geben.

Der erste Abschnitt gibt einen Überblick über die verfassungsrechtlichen Grundlagen und die Regelungssystematik. Erläuterungen zu den wichtigsten rechtlichen Datenverarbeitungsbedingungen enthält der zweite Abschnitt. Im dritten Abschnitt sind die einschlägigen Vorschriften des Schulgesetzes, die Rechtsverordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 sowie die im Jahr 2009 vom Hessischen Kultusministerium ergangenen Erlasse zur Verarbeitung personenbezogener Daten abgedruckt. Das **Hessische Datenschutzgesetz**, die aktuelle Fassung des im vergangenen Jahr umfassend novellierten **Bundesdatenschutzgesetzes** sowie **Art. 1 und 2 des Grundgesetzes** runden das Werk mit den Vorschriften zum allgemeinen Datenschutzrecht ab..

Wiesbaden, im Januar 2010

Professor Dr. Michael Ronellenfitsch

I. Warum besondere Datenverarbeitungsregelungen für Schulen?

Nebeneinander von Hessischem Datenschutzgesetz, Schulgesetz und Verordnungsrecht

Wer das Hessische Datenschutzgesetz vom 7. Januar 1999 kennt, wird sich vielleicht fragen: Warum überhaupt spezielle Datenverarbeitungsvorschriften für Schulen - genügen nicht die allgemeinen Bestimmungen des Hessischen Datenschutzgesetzes? Dort ist doch bereits geregelt, dass Behörden zur rechtmäßigen Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten dürfen und welche Grenzen bei der Erhebung, Speicherung, Verwendung und Übermittlung der Daten zu beachten sind.

Fragt man nach dem rechtlichen Hintergrund des Datenschutzes, sind zwei Wurzeln maßgebend, die gesetzliche Begrenzung staatlicher Befugnisse und die bürgerlichen Freiheitsrechte. Die grundlegenden Antworten sind vom **Bundesverfassungsgericht** im so genannten Volkszählungsurteil von 1983 formuliert worden. In seiner für den Datenschutz wichtigsten Entscheidung hat es aus dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz gewährleisteten allgemeinen Persönlichkeitsrecht das **Recht auf informationelle Selbstbestimmung** abgeleitet. Es ist die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfGE 65, 1 und 43). Jede Erhebung und weitere Verarbeitung personenbezogener Daten durch staatliche Behörden - dazu gehören auch die öffentlichen Schulen - ist somit ein **Grundrechtseingriff**. Öffentliche Stellen dürfen nur in Grundrechte eingreifen, wenn eine Rechtsvorschrift dies eindeutig erlaubt und präzise umschreibt. Ähnliche Grundsätze sind im Bundesdatenschutzgesetz für private Schulen normiert worden (§§ 28 ff. BDSG).

Die verfassungsrechtlichen Schranken sind entscheidend für die Ausgestaltung der gesetzlichen und verordnungsrechtlichen Vorgaben. Je schwerwiegender der Eingriff in das informationelle Selbstbestimmungsrecht ausfällt, desto dringlicher erscheint die Notwendigkeit, die Einzelheiten der staatlichen Datenverarbeitung in speziellen Rechtsvorschriften festzulegen (Gebot „normenklarer“ gesetzlicher Erlaubnisse). Das allgemein geltende HDSG kann auf viele regelungsbedürftige Einzelheiten der Datenverarbeitung in den Schulen naturgemäß nicht eingehen, so dass es im Schulrecht zu bereichsspezifischen Sonderregelungen gekommen ist.

Zu den schwerwiegenden Eingriffen zählt das Bundesverfassungsgericht ausdrücklich die Fälle, in denen der Staat vom Bürger die Offenbarung personenbezogener Daten verlangt. Ein Zwang zur Preisgabe personenbezogener Daten setzt aber voraus, dass der Gesetzgeber den besonderen Verwendungszweck präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Diese Situation entsteht bei der Einschulung des Kindes und auch im späteren Schulleben. Deswegen werden Eltern verpflichtet, der Schulverwaltung eine Reihe von persönlichen Daten über sich selbst und ihr Kind zur Verfügung zu stellen. Auch die wiederkehrende Abfrage der schulischen Leistungsfähigkeit der Schülerinnen und Schüler zählt dazu. Mit den besonderen Datenverarbeitungsnormen des Schulgesetzes und den ergänzenden

Vorschriften des Hessischen Datenschutzgesetzes hat der Hessische Landtag die Anforderungen erfüllt, die das Bundesverfassungsgericht an eine verfassungskonforme Verarbeitung personenbezogener Daten stellt.

Das **Hessische Datenschutzgesetz** (HDSG) wird damit freilich nicht bedeutungslos für den Schulbereich. Bei der Datenverarbeitung in den Schulen stellen sich oft die gleichen Fragen wie in anderen Verwaltungsbereichen. Wo das Schulgesetz und die dazu ergangenen Verordnungen keine spezifische Antwort geben, finden die allgemeinen Vorschriften des HDSG ergänzende Anwendung. So definiert § 2 Abs. 1 und 2 HDSG und nicht das Schulgesetz, was als Verarbeitung personenbezogener Daten anzusehen ist. Auch die Zusammenstellung der Rechte der von der Datenverarbeitung Betroffenen (auf Datenberichtigung, Löschung, Kontrolle, Schadensersatz etc.) ergibt sich allein aus dem HDSG. Die Kontrollbefugnisse, die der Hessische Datenschutzbeauftragte gegenüber den Schulen hat, sind ebenfalls ausschließlich im HDSG festgelegt. All das folgt aus der Anordnung des Gesetzgebers in § 83 Abs. 8 des Schulgesetzes, dass das Hessische Datenschutzgesetz anzuwenden ist, soweit das Schulgesetz nichts Besonderes regelt.

Das Schulgesetz wird nicht nur durch die allgemeinen Vorschriften des HDSG ergänzt. Manche der Vorgaben für die Datenverarbeitung in den Schulen müssen so detailliert sein und müssen unter Umständen auch verhältnismäßig kurzfristig an geänderte Verhältnisse angepasst werden können, dass ein Parlamentsgesetz kein geeignetes Regelungsinstrument wäre. § 83 Abs. 9 des Schulgesetzes enthält deswegen eine Ermächtigung an das Kultusministerium „Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule“ näher in einer Rechtsverordnung zu regeln. Deshalb findet man z.B. die Bedingungen, unter denen Lehrerinnen und Lehrer auf privaten PC außerhalb der Schule personenbezogene Schülerdaten verarbeiten dürfen, in der **Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen**. Aus dem gleichen Grund bestimmt diese Rechtsverordnung des Kultusministeriums auch die einzelnen Daten, welche die Schule über Erziehungsberechtigte, Schülerinnen und Schüler speichern darf.

Wer sich mit Datenschutz in der Schule beschäftigt, muss sich also mit dem Schulgesetz, der Rechtsverordnung dazu und dem Hessischem Datenschutzgesetz vertraut machen.

II. Die wichtigsten rechtlichen Datenverarbeitungsbedingungen

1. Anwendungsbereich der Datenschutzvorschriften: Schulen in freier und kirchlicher Trägerschaft

Auf Schulen in freier Trägerschaft finden die Datenschutzbestimmungen des Schulgesetzes im Allgemeinen keine Anwendung. Ausnahmen sind § 71 Abs. 6, der den Anwendungsbereich der Vorschriften zur Schulgesundheitspflege und zum schulpsychologischen Dienst auf Schulen in freier Trägerschaft ausdehnt, und § 72 Abs. 6, der auch den Schülerinnen und Schülern an diesen Schulen und den Erziehungsberechtigten ein Akteneinsichtsrecht gemäß § 72 Abs. 5 gewährt.

Für die Datenverarbeitung der Schulen in **evangelischer Trägerschaft** gilt das Kirchengesetz über den Datenschutz an der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (ABl. EKD 1993 S. 505); geändert durch Kirchengesetz vom 7. November 2002 (ABl. EKD 2002 S. 381). Schulen in **römisch-katholischer Trägerschaft** müssen sich an die „Anordnung über den kirchlichen Datenschutz der katholischen Kirche“ vom 14. Oktober 2003 halten (Kirchliches Amtsblatt für die Diözese Münster Nr. 24 vom 15. Dezember 2003, S. 294).

2. Verarbeitungsbefugnisse der Schulen, der Schulaufsichtsbehörden und der Schulträger

§ 83 Abs. 1 und 2 HSchulG

(1) Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, soweit die Kenntnis der Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist.

(2) Schulträger und Schulaufsichtsbehörden dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben der Schulplanung, der Schulorganisation und der Schulaufsicht und einem jeweils damit verbundenen Zweck oder zur Durchführung organisatorischer Maßnahmen erforderlich ist. Abs. 1 Satz 2 gilt entsprechend.

§ 83 ist die zentrale Bestimmung für die Verarbeitung personenbezogener Daten in Schulen, Schulaufsichtsbehörden und beim Schulträger. Hier ist festgelegt, für welche Aufgaben und Zwecke auch **ohne Einwilligung** der Schülerinnen und Schüler, Erziehungsberechtigten und Lehrer deren persönliche Daten verarbeitet werden dürfen. Datenverarbeitung außerhalb dieses Rahmens ist nur mit ausdrücklicher Einwilligung

der Betroffenen zulässig. Dies folgt aus § 7 Abs. 1 HDSG, denn danach ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie aufgrund einer Rechtsvorschrift erfolgt oder der Betroffene eingewilligt hat.

Wie das gesamte Datenschutzrecht gelten auch die einschränkenden Datenverarbeitungsnormen des Schulgesetzes nur für die Verarbeitung **personenbezogener Daten**. Was unter personenbezogenen Daten zu verstehen ist, definiert das HDSG. Es sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die in der Terminologie des Datenschutzrechts als „**Betroffener**“ bezeichnet wird (vgl. § 2 HDSG). Aggregierte Datensammlungen und -auswertungen, die keine Angaben enthalten, welche einer einzelnen Person zugeordnet werden können (so genannte anonymisierte oder pseudonymisierte Daten), sind somit keine personenbezogenen Angaben und unterliegen daher nicht dem Datenschutz. Datenschutzrechtlich zu überprüfen ist allerdings, ob Anonymisierung oder Pseudonymisierung sichergestellt sind, insbesondere ob personenbezogene Merkmale sauber von den Daten getrennt sind, die in die Datenbank eingehen. Ein Beispiel bietet die Ermittlung des Notendurchschnitts aller Abiturienten einer Klasse oder Schule. **Bestimmbar** ist eine Person, wenn mit erreichbarem Zusatzwissen eine Identifizierung möglich ist. Das ist etwa der Fall, wenn die Schulaufsichtsbehörde der Presse mitteilt, dass gegen den Geschichtslehrer einer bestimmten Schule ein Disziplinarverfahren eingeleitet worden sei.

Eine Datenverarbeitung, die ohne Einwilligung der Betroffenen erfolgt, muss für die in § 83 Abs. 1 und 2 bestimmte **Aufgabenerfüllung** erforderlich sein. Dazu gehören in den Schulen alle Erhebungen und Verarbeitungen, die zur Erfüllung des gesetzlichen Bildungs- und Erziehungsauftrages und zur Abwicklung schulorganisatorischer Maßnahmen erforderlich sind. Die Schule benötigt beispielsweise die Namen und Adressen der gewählten Klassenelternbeiräte, um diese über schulische Belange zu informieren. In den Schulaufsichtsbehörden und bei den Schulträgern sind die Zwecke der Datenverarbeitungen deutlich enger gezogen; sie müssen zur Schulplanung, Schulorganisation und Schulaufsicht erforderlich sein. Insofern werden nur in Ausnahmefällen personenbezogene Daten erforderlich sein. Meist dürften anonymisierte oder pseudonymisierte Daten ausreichen. Es genügt nicht, dass die Datenverarbeitung nützlich ist, sondern sie ist nur zulässig, wenn die Aufgabe sonst nicht erfüllt werden kann. In der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. Nr. 4/2009 S. 131) ist präzisiert, welche Angaben für die Schulen erforderlich sind (vgl. § 1 Abs. 1 und die Anlagen 1, 2 und 3 der Verordnung). Neben dem Katalog der zur Verarbeitung zugelassenen Schüler- und Lehrerdaten ist dort auch der zulässige Inhalt des Klassenbuchs festgelegt.

Da die Datenschutzvorschriften die freie Entfaltung der Persönlichkeit schützen sollen, gelten sie nicht für die Daten **Verstorbener**. Deren Daten sind freilich nicht schutzlos, denn die durch Art. 1 Abs. 1 Grundgesetz geschützte Würde eines Menschen darf auch nach dessen Tod nicht verletzt werden.

Mit „**Verarbeiten“** ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener Daten gemeint, siehe dazu die Definition in § 2 Abs. 2 HDSG. In dieser

Vorschrift sind auch die verschiedenen Phasen der Verarbeitung (Erheben, Speichern, Übermitteln, Sperren und Löschen) näher beschrieben.

3. Pflicht zur Mitwirkung bei der Datenerhebung und Information über den Zweck der Datenverarbeitung

§ 83 Abs. 3 HSchulG

Schülerinnen und Schüler, deren Eltern und Lehrerinnen und Lehrer sind verpflichtet, die erforderlichen Angaben zu machen.

Tritt die Schülerin oder der Schüler in das Schulverhältnis ein - im Rahmen der Einschulung oder nach einem Schulwechsel -, benötigt die Schulverwaltung von ihm/ihr und den Eltern eine Reihe von Informationen, die für die Schulverwaltung unverzichtbar sind. Da die meisten Angaben nur von den Erziehungsberechtigten oder den Schülerinnen und Schülern gemacht werden können, ist ihre Mitwirkung unabdingbar. Der Katalog der Daten ist in Anlage 1 der Verordnung abschließend festgelegt.

Das Hessische Datenschutzgesetz enthält in § 12 Abs. 4 u.a. das Gebot, die Betroffenen bei der Datenerhebung in geeigneter Weise über den Zweck der Datenerhebung und die Rechtsgrundlage einer eventuell bestehenden Auskunftspflicht zu informieren. Um diesem Gebot gerecht zu werden, hat das Hessische Kultusministerium mit Erlass vom 19. Oktober 2009 ein Merkblatt zur Verfügung gestellt, mit dem Eltern bzw. volljährige Schülerinnen und Schüler über die Verarbeitung ihrer Daten informiert werden.

Der Erlass und das Merkblatt ist bei den Materialien unter Abschnitt III Ziff. 1.3.2 abgedruckt. Die Veröffentlichung im Amtsblatt des Hessischen Kultusministeriums (ABl. 2009 S. 811) erfolgte in vier Sprachen (deutsch, englisch, arabisch und türkisch).

§ 71 Abs. 1 und 2 HSchulG

(1) Soweit zur Vorbereitung einer Entscheidung nach diesem Gesetz schulärztliche oder schulpsychologische Untersuchungen sowie sonderpädagogische Überprüfungen erforderlich werden, sind die Kinder, Jugendlichen und volljährigen Schülerinnen und Schüler verpflichtet, sich untersuchen zu lassen und an wissenschaftlich anerkannten Testverfahren teilzunehmen.

(2) Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler haben die für die Untersuchungen erforderlichen Angaben zu machen. Kinder, Jugendliche und volljährige Schülerinnen und Schüler dürfen dabei in der Regel nicht befragt werden über Angelegenheiten, die ihre oder die Persönlichkeitssphäre ihrer Eltern oder Angehörigen betreffen.

In verschiedenen Entscheidungsprozessen nach dem Schulgesetz, z.B. bei der Prüfung des Vorliegens des sonderpädagogischen Förderbedarfs nach § 54 Abs. 1 HSchulG sind ausdrücklich schulärztliche und schulpsychologische Untersuchungen notwendig. Hierzu legt § 71 Abs. 1 und 2 ausdrücklich fest, dass die Betroffenen an diesen Untersuchungen, die oftmals zu sensiblen Daten führen, teilnehmen müssen und zur Auskunft in erforderlichem Maße verpflichtet sind. Ohne eine solche gesetzliche Verpflichtung bliebe es bei der Freiwilligkeit. Sonstige Erhebungen und wissenschaftliche Untersuchungen sind nur durchführbar, soweit die Schülerinnen und Schüler oder ihre Erziehungsberechtigten nach voller Aufklärung über die Freiwilligkeit eingewilligt haben.

4. Automatisierte Datenverarbeitung

§ 83 Abs. 6 Satz 4 und Satz 5 HSchulG

Medizinische Befunde dürfen nicht automatisiert verarbeitet werden, ausgenommen die medizinischen Befunde der für die Schulgesundheitspflege zuständigen Behörden (§ 149). Personenbezogene Daten des schulpsychologischen Dienstes dürfen nur automatisiert verarbeitet werden, wenn sie dabei nach dem jeweiligen Stand der Technik hinreichend sicher verschlüsselt werden.

Das in § 83 Abs. 4a HSchulG alter Fassung noch enthaltene umfassende Verbot der automatisierten Verarbeitung von medizinischen Daten der Schülerinnen und Schüler ist nunmehr eingeschränkt worden. Von „automatisierter Datenverarbeitung“ spricht man, sobald die Datenverarbeitung unter Einsatz von PC und Servern erfolgt (s. § 2 Abs. 6 HDSG). Zulässig ist die Verarbeitung jener medizinischen Daten, die die Gesundheitsämter der Schulträger erhoben haben, soweit sie im Rahmen der Schulgesundheitspflege erforderlich sind.

Auch den Schulpsychologen in den staatlichen Schulämtern ist es nun erlaubt, die von ihnen erhobenen Daten automatisiert zu verarbeiten, allerdings mit der Auflage einer hinreichend sicheren Verschlüsselung, die dem Stand der Technik entsprechen muss. Die DV kann auf dem Server des Schulamts erfolgen, wenn die Verschlüsselung sicherstellt, dass nur der zuständige **Schulpsychologe Zugriff erlangen kann.**

§ 83 Abs. 7 HSchulG

Die automatisierte Verarbeitung personenbezogener Daten darf in der Schule nur mit schuleigenen Datenverarbeitungsgeräten erfolgen, es sei denn, dass die Beachtung der erforderlichen Datensicherheitsmaßnahmen gewährleistet ist.

§ 83 Abs. 9 HSchulG

Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule werden durch Rechtsverordnung näher geregelt; dabei ist zu bestimmen, welche Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten außerhalb der Schule zu berücksichtigen sind.

In § 2 der Rechtsverordnung ist die Organisation der Datenverarbeitung näher geregelt.

§ 2 der Verordnung zur Verarbeitung personenbezogener Daten in Schulen und statistischen Erhebungen an Schulen

(1) Anlagen zur Verarbeitung personenbezogener Daten in Schulen dürfen mit Datenverarbeitungseinrichtungen für Unterrichtszwecke nur vernetzt werden, wenn eine zuverlässige Trennung der Daten gewährleistet ist. Nach § 10 Abs. 2 Satz 2 des Hessischen Datenschutzgesetzes muss jede Schule ein IT-Sicherheitskonzept erstellen.

(2) Geräte zur Verarbeitung personenbezogener Daten dürfen nur an Einrichtungen zur elektronischen Kommunikation angeschlossen werden, wenn die in dem Gerät gespeicherten personenbezogenen Daten durch geeignete Maßnahmen gegen unberechtigten Zugriff geschützt werden.

(3) Bei der Datenverarbeitung in Schulen sind die Standards der von dem Bundesamt für Sicherheit in der Informationstechnik für den IT-Grundschutz veröffentlichten Regeln einzuhalten.

Da bei der praktischen Umsetzung des § 2 in den Schulen erhebliche Schwierigkeiten auftraten, hat das Hessische Kultusministerium mit dem Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen, zur Nutzung von E-Mail und Erhebung und Veröffentlichung interner Daten vom 27. November 2009 (s. Seite 71 dieser Broschüre; Veröffentlichung im Amtsblatt im Jahr 2010) weitere Details zur IT-Sicherheit festgelegt.

Der Erlass beschäftigt sich mit der Trennung des Verwaltungsnetzes vom pädagogischen Netz (§ 2 Abs. 1 Satz 1), enthält wichtige Elemente eines Sicherheitskonzeptes (§ 2 Abs. 1 Satz 2) und regelt den Anschluss der Schulnetze an das Internet (§ 2 Abs. 2) unter Berücksichtigung der Standards des BSI (§ 2 Abs. 1 Satz 3).

5. Verarbeitung von Schüler- oder Elterndaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

5.1 Rechtliche Rahmenbedingungen

§ 83 Abs. 9 HSchulG

Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule

werden durch Rechtsverordnung näher geregelt; dabei ist zu bestimmen, welche Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten außerhalb der Schule zu berücksichtigen sind.

Dem Gebot Umfang und Einzelheiten der personenbezogenen Datenverarbeitung näher zu regeln und dabei auch die Sicherheitsmaßnahmen zu bestimmen, die bei der Datenverarbeitung außerhalb der Schule zu berücksichtigen sind, ist das Kultusministerium mit der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. 2009 S. 131 – s. Teil III Ziff. 1.2) nachgekommen. Damit hat es gegenüber der Vorfassung der Verordnung aus dem Jahre 1993 eine modernisierte Rechtsgrundlage für die Datenverarbeitung in Schulen geschaffen.

Das Hessische Kultusministerium hat mit Erlass vom 21. August 2009 (ABl. 2009 S. 726 – s. Teil III Ziff. 1.3.1) weitere Details für die IT-Sicherheit am heimischen Arbeitsplatz der Lehrkräfte festgelegt, ein Formblatt zur Anmeldung des häuslichen Arbeitsplatzes herausgegeben und Handreichungen zur Umsetzung der Vorgaben des Erlasses erteilt.

Mit § 1 Abs. 5 und § 3 der Verordnung werden die grundlegenden Voraussetzungen für die Verarbeitung der Daten von Schülern und Eltern auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte vorgegeben. Denn egal wo die Datenverarbeitung stattfindet, ob in der Wohnung der Lehrkraft oder in der Schule und egal, ob auf einem privaten oder von der Behörde beschafften Computer, es bleibt eine Datenverarbeitung der Schule. Die Verantwortung über die Rechtmäßigkeit der Datenverarbeitung verbleibt bei ihr (§ 3 Abs. 5). Damit die Schulleitung überhaupt davon Kenntnis hat wofür sie die Verantwortung trägt, verlangt § 3 Abs. 1 eine schriftliche Anzeige der Lehrkraft. Die Anzeige muss bestimmte Angaben enthalten und es dürfen nur ganz bestimmte in Anlage 1 Ziffer A.6 der Verordnung abschließend aufgezählte Daten verarbeitet werden. Der Erlass enthält als Anlage 1 ein Formblatt, mit dem die Datenverarbeitung anzeigt werden kann. Die Erklärung orientiert sich an den Standards für die Datenverarbeitung außerhalb der Daten verarbeitenden Stelle. Maßgeblich war hier die Vereinbarung zur dauerhaften Einführung alternierender Telearbeit im Bereich der Hessischen Landesverwaltung. Die Erklärung enthält daher auch eine Passage, wonach die Lehrkraft sich verpflichtet, auch zu Hause das Hessische Datenschutzgesetz zu beachten und die Voraussetzungen für eine Kontrolle des Hessischen Datenschutzbeauftragten sicherzustellen.

§ 3 Abs. 2 und 3 der Verordnung verlangen, dass die personenbezogenen Daten nach Ende des Datenverarbeitungsvorganges bzw. nach Abschluss der Aufgabe ggf. unverzüglich in die Schüler- oder Schulaktenführung zu nehmen, ansonsten auf den automatisierten Anlagen zu löschen sind.

§ 3 Abs. 4 der Verordnung widmet sich den sonderpädagogischen Gutachten. Wegen des besonders starken Eingriffes in die Grundrechte der Betroffenen sind dabei auch besondere Maßnahmen zu Datensicherheit zu treffen. Das Erfordernis wird deutlich, wenn man sich den normenklar und transparent nachzulesenden Katalog der in Frage kommenden Daten in der Anlage 1 A Ziff. 6.14 ansieht. Informationen zur Anamnese

des Schülers in seiner Familie, zur Vorgeschichte, zum Lernverhalten, zur sprachlichen und körperlichen Entwicklung, zum emotionalen und sozialen Verhalten und Weiteres darf zu diesem Zweck verarbeitet werden. Folgerichtig verlangt § 3 Abs. 4 besondere Maßnahmen zu treffen, um diese Daten gegen den unberechtigten Zugriff zu schützen.

In § 3 Abs. 6 der Verordnung wird der Schulleitung die Befugnis eingeräumt der Lehrkraft die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungseinrichtungen zu untersagen, wenn gegen die Verordnung oder das Datenschutzgesetz verstoßen wird.

5.2 Technische und organisatorische Maßnahmen

Der Erlass fordert konsequent, dass die Speicherung der personenbezogenen Daten auf einem separaten verschlüsselten Datenträger erfolgt, der ausschließlich für diese Zwecke verwendet wird. Neben den hier gemeinten USB-Geräten ist auch eine durch Verschlüsselung und Zugriffsmechanismen geschützte individuelle (lehrkraftbezogene) Speicherung der Daten auf einer ggf. vorhandenen Plattform der Schule oder des Schulträgers möglich.
Bei der zur Verschlüsselung verwendeten Software für die USB-Komponenten, ist darauf zu achten, dass ein sicherer Algorithmus verwendet wird und dass Dateien möglichst nicht einzeln verschlüsselt werden, sondern besser in einem verschlüsselten Container, und damit in einem nur für den jeweils Berechtigten einsehbaren Verzeichnis abgelegt werden.

5.2.1 Allgemeine Schüler- und Elterndaten

Zum Schutz der Schüler- und Elterndaten mit normalem Schutzbedarf nach Anlage 6 Punkt 1 - 13 der Rechtsverordnung vor unbefugtem Zugriff und zur Sicherstellung der Verfügbarkeit sind die Lehrkräfte durch die Schulen über die Verarbeitungsbedingungen zu unterrichten und auf die Einhaltung der folgenden organisatorischen und technischen Maßnahmen zu verpflichten:

Die Lehrkräfte melden die Verarbeitung der Daten bei ihrer Schule an und hinterlegen für Notfälle das persönliche Passwort für die Verschlüsselung in einem verschlossenen Umschlag, der in der Schule gesichert aufbewahrt wird.

Arbeitsergebnisse sind zeitnah auf die Systeme der Schulverwaltung zu übertragen. Werden Arbeiten in mehreren Schritten vervollständigt oder über längere Zeiträume fortgeführt, sind dort auch regelmäßig Sicherungskopien zu hinterlegen.

Daten, die nach der Übertragung in die Systeme der Schulverwaltung nicht mehr lokal benötigt werden, sind, soweit die Aufbewahrung nicht explizit geregelt ist, unverzüglich zu löschen. Wenn aus vorhandenen Schriftstücken durch Löschen der Personenbezüge Textbausteine gewonnen werden, ist darauf zu achten, dass die personenbezogenen Daten nicht über die Historiefunktion der Office-Software mitgespeichert werden.

Der häusliche Arbeitsplatz ist so einzurichten, dass Daten und Unterlagen von Unbefugten nicht eingesehen werden können.

Sämtliche Unterlagen sind außerhalb der Bearbeitungsphase verschlossen aufzubewahren.

Es ist den Lehrkräften untersagt, die verarbeiteten Daten auf den lokalen Festplatten ihres Systems oder anderen Datenträgern oder Plattformen, als den dafür vorgesehenen, abzulegen. Um sicherzustellen, dass auch nach Programmabstürzen keine unbemerkten lokalen Kopien entstehen, müssen die temporären Verzeichnisse nach jeder Verarbeitung überprüft und ggf. bereinigt werden.
Unerledigte Druckaufträge sind zu löschen.

Wird die Bearbeitung unterbrochen, ist der Zugang zum Rechner und insbesondere zu den Daten zu sperren. Ggf. ist eine Benutzerabmeldung durchzuführen. Zusätzlich ist die automatische Sperrfunktion mit Passwortschutz am Bildschirmschoner auf eine Inaktivität von höchstens 15 Minuten Dauer einzustellen.

Der eingesetzte Rechner muss durch einen tagesaktuellen Virenscanner geschützt werden.

Ist der Rechner in ein privates Netzwerk eingebunden, sind unbefugte Zugriffe durch geeignete Konfigurationen oder durch physikalisches Trennen auszuschließen. Bei besonders gefährdeten Schnittstellen, wie WLAN sind sichere Verschlüsselungsmechanismen zu aktivieren.

Während der Verarbeitung der unverschlüsselten Daten am häuslichen System muss jede Verbindung in das Internet aktiv unterbrochen werden.

5.2.2 Sonderpädagogische Gutachten

Bei den in § 3 Absatz 4 der Rechtsverordnung genannten Daten (s. auch Anlage 1 A Ziff. 6.14), die im Zusammenhang mit der Erstellung von sonderpädagogischen Gutachten anfallen, ist ein höherer Schutzbedarf gegeben.

Gerade für die Verarbeitung dieser Daten ist der Einsatz dienstlicher Geräte anzustreben.

Wenn dies nicht zu realisieren ist, sind für das Erstellen von Fördergutachten mit privaten Geräten Verfahren zu wählen bzw. zu entwickeln, die jede Speicherung der Daten auf den privaten Datenverarbeitungsgeräten der Lehrkräfte weitgehend technisch ausschließen und deren Wirkung nicht von einem störungsfreien Betrieb und der Umsetzung organisatorischer Maßnahmen abhängig ist.

Daher dürfen die oben beschriebenen, plattformbasierten Lösungen in diesem Fall keine Download-Funktion haben, damit die Fördergutachten nicht auf das lokale System übertragen werden können. Zwischen den Prozessen auf der Plattform und dem lokalen

System ist dann auch ein "Kopieren und Einfügen" zu unterdrücken, wie es z.B. bei Terminalserver-Lösungen möglich ist. Ein Ausdruck der Fördergutachten kann dann ausschließlich in der Schule an einem Drucker erfolgen, der über eine entsprechende netztechnische Anbindung mit der Plattform verbunden ist.

USB-Geräte kommen hier nur in bootfähiger Ausführung in Betracht. Dabei ist durch den Bootvorgang sicherzustellen, dass die lokalen Speichermedien, wie z.B. die Festplatte oder die Netzwerk-Schnittstellen, nicht in die Systemumgebung eingebunden werden. Eine Bearbeitung der Fördergutachten erfolgt dann zwingend nur auf dem zugelassenen USB-Gerät im verschlüsselten Container. Darüber hinaus kann noch die Schnittstelle zum Drucker aktiviert werden, damit die in der Rechtsverordnung vorgesehene Endfassung des Dokumentes erstellt werden kann.

Diese besonderen Maßnahmen sind wegen der besonderen Eingriffstiefe in die Rechte der Betroffenen verhältnismäßig. Das Hessische Kultusministerium verweist dazu in seinem Erlass auf die Homepage meiner Behörde. Unter der Rubrik „Fachthemen/Datenschutz in Schulen“ unter dem Titel „Verarbeitung von Schüler- und Lehrerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte“ können diese besonderen, dem technischen Wandel unterliegenden Maßnahmen eingesehen werden. Sie sind hier zum Stand Dezember 2009 wiedergegeben.

6. Forschung im Schulbereich

§ 84 HSchulG

(1) Wissenschaftliche Forschungsvorhaben in Schulen bedürfen der Genehmigung des Kultusministeriums; die Befugnis kann auf die Schulaufsichtsbehörden übertragen werden. Die Genehmigung erziehungswissenschaftlicher Forschungsvorhaben soll erteilt werden, wenn die Erfüllung des Bildungsauftrages der Schule hierdurch nicht unangemessen beeinträchtigt wird. Vor Erteilung der Zustimmung ist die Schulkonferenz zu hören. Die Genehmigung von Forschungsvorhaben, bei denen personenbezogene Daten verarbeitet werden, ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Personenbezogene Daten dürfen für ein bestimmtes wissenschaftliches Forschungsvorhaben in der Regel nur mit Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler verarbeitet werden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Personenbezogene Daten dürfen ohne Einwilligung der Betroffenen verarbeitet werden, soweit deren schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung der Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung ohne Rechtsnachteile verweigern können; sie sind dabei über das Ziel und den wesentlichen Inhalt des Forschungsvorhabens, die Art ihrer Beteiligung an der Untersuchung sowie

die Verarbeitung der erhobenen Daten aufzuklären. § 33 Abs. 2 und 3 HDSG in der Fassung vom 7. Januar 1999 (GVBl. I S. 98) gilt entsprechend.

(3) Abs. 2 gilt entsprechend für Untersuchungen in Schulen, die vom Kultusministerium oder in dessen Auftrag durchgeführt werden.

Die Vorschrift ergänzt die Forschungsregelung in § 33 HDSG. Die dort zu findende **Privilegierung** der Verarbeitung personenbezogener Daten für Forschungszwecke hat der Gesetzgeber im Schulgesetz noch etwas erweitert und gleichzeitig die Informationspflichten der Forscher präzisiert. Während die HDSG-Vorschrift nur die Übermittlung von Daten regelt, erfasst § 84 Abs. 2 HSchulG sämtliche Verarbeitungsformen. Das bedeutet: Unter den gleichen erleichterten Voraussetzungen, unter denen die Schulen aufgrund des HDSG bislang schon Daten zu Forschungszwecken weitergeben durften, können Forschungseinrichtungen jetzt selbst Erhebungen in Schulen durchführen.

Personenbezogene Daten der Schülerinnen und Schüler und Erziehungsberechtigten dürfen normalerweise nur mit deren Einwilligung für Forschungszwecke verarbeitet werden. Zu beachten ist hier, dass die Eltern auch für Minderjährige ab 14 Jahren noch die Einwilligung erteilen müssen. Die Einwilligung selbst muss den Anforderungen des § 7 Abs. 2 HDSG entsprechen. Ihr muss die Aufklärung über die dort genannten Punkte vorangehen und sie muss schriftlich erfolgen.

Eine Einwilligung ist nicht erforderlich, soweit aus den im Gesetz genannten Gründen keine schutzwürdigen Belange der Betroffenen beeinträchtigt werden. In Betracht kommen könnte hier beispielsweise die Mitteilung von Namen und Anschriften der Erziehungsberechtigten an ein unabhängiges Forschungsinstitut, das im Rahmen eines erziehungswissenschaftlichen Forschungsprojekts eine Befragung durchführen möchte.

Die Einwilligung ist mitunter schon aus rein technischen Gründen nicht oder nur schwer zu erlangen, etwa wenn die betroffenen Schülerinnen und Schüler die Schule bereits verlassen haben. Zuweilen könnte der Forschungszweck gefährdet werden, müsste die Einwilligung der Betroffenen eingeholt werden. Das ist beispielsweise bei Forschungsprojekten möglich, bei denen es auf die Beobachtung des unbefangenen, spontanen Verhaltens der Schülerinnen und Schüler ankommt.

Deshalb gestattet das Gesetz in Ausnahmefällen einen Verzicht auf das Erfordernis der Einwilligung, obgleich schutzwürdige Belange der betroffenen Schülerinnen und Schüler und Erziehungsberechtigten beeinträchtigt werden. Die Schülerinnen und Schüler und Erziehungsberechtigten müssen die Beeinträchtigung allerdings nur hinnehmen, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens ihre schutzwürdigen Belange erheblich überwiegt. Beispiel: Das Kultusministerium möchte die Effektivität neuer Unterrichtsformen durch eine wissenschaftliche Begleitforschung überprüfen lassen. Darüber, was „**wissenschaftliche Forschung“** ist, lässt sich trefflich streiten. Die Literatur zu diesem Thema füllt Bibliotheken. Empfehlenswert dürfte sein, sich an der sehr weiten Begriffsbestimmung des Bundesverfassungsgerichts zu orientieren. Das Gericht lässt alles genügen, „was nach Inhalt und Form als ernsthafter,

planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist“ (BVerfGE 35, S. 113; 47, S. 367). Eine Diplomarbeit würde diese Anforderungen bereits erfüllen.

Verfahrensrechtlich ist zu beachten, dass das wissenschaftliche Forschungsprojekt stets vorab vom Hessischen Kultusministerium – nach Anhörung der Schulkonferenz – zu genehmigen ist. Der Hessische Datenschutzbeauftragte erhält eine Kopie des Genehmigungsschreibens bei personenbezogenen Forschungsprojekten.

In Ergänzung der gesetzlichen Bestimmungen ist der Erlass des Hessischen Kultusministeriums vom 27. Februar 1997 zu Wissenschaftlichen Forschungen im Schulbereich zu beachten (ABl. 1997 S. 186).

7. Ordnungsmaßnahmen

§ 82 Abs. 10 HSchulG

Eintragungen und Vorgänge über Ordnungsmaßnahmen sind spätestens am Ende des zweiten Schuljahres nach der Eintragung zu löschen, sofern nicht während dieser Zeit eine erneute Ordnungsmaßnahme getroffen wurde.

Das Schulgesetz sieht in § 82 eine Reihe von Ordnungsmaßnahmen vor. Die mildeste Maßnahme ist der Ausschluss vom Unterricht für den Rest des Schultages, die härteste die Verweisung von der Schule. Dazwischen gibt es mehrere abgestufte Sanktionsmöglichkeiten, wie etwa die Androhung der Zuweisung in eine Parallelklasse oder die Androhung der Überweisung in eine andere Schule.

Die Dokumentation dieser Maßnahmen in der Schülerakte ist notwendig. Sie ist allerdings ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung, der nach der Rechtsprechung des Bundesverfassungsgerichts besondere Grundrecht sichernde verfahrenstechnische Vorkehrungen erfordert. Deshalb enthält Abs. 10 eine **Tilgungsvorschrift**. Eintragungen und Vorgänge über Ordnungsmaßnahmen müssen spätestens am Ende des zweiten Schuljahres nach der Eintragung gelöscht werden, wenn nicht während dieser Zeit erneut eine Maßnahme getroffen wurde.

Die gesetzliche Regelung ist erfolgt, damit das Löschungsgebot von den Schulen künftig genau eingehalten wird. Die gleiche Pflicht ergibt sich aus der Verordnung über das Verfahren bei Ordnungsmaßnahmen vom 8. Juli 1993 (ABl. 2000 S. 688, geändert durch Verordnung vom 14. Dezember 1999 (ABl. 2000 S. 3).

8. Informationsrechte der Schülerinnen, Schüler und Erziehungsberechtigten

§ 72 Abs. 4 HSchulG

Die Eltern volljähriger Schülerinnen und Schüler sind bis zur Vollendung des 21. Lebensjahres über wesentliche, das Schulverhältnis betreffende Sachverhalte, insbesondere über Versetzungsgefährdungen und Nichtversetzungen sowie über Ordnungsmaßnahmen nach § 82 Abs. 2 Nr. 5 bis 8 und Abs. 8 zu informieren, sofern die volljährige Schülerin oder der volljährige Schüler dem nicht widersprochen hat. Über den Widerspruch werden die Eltern von der Schule informiert. Die Schülerinnen und Schüler sind auf diese Regelung hinzuweisen.

§ 72 Abs. 5 HSchulG

Jugendliche, die Eltern und volljährige Schülerinnen und Schüler haben das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter derart verbunden sind, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist den Betroffenen über die zu ihrer Person gespeicherten Daten Auskunft zu erteilen.

Die Bürgerinnen und Bürger haben einen Anspruch darauf zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“. Das verlangt das Bundesverfassungsgericht im Volkszählungsurteil von 1983 (BVerfGE 65, 1, 43). Das ist fraglos nur möglich, wenn sie von der Behörde Auskunft hinsichtlich der über sie gespeicherten Daten verlangen oder - noch besser - Einsicht in die einschlägigen Akten nehmen können. Geht es um eine konkrete Verwaltungsentscheidung, also beispielsweise um eine Versetzung, gewährt § 29 HVwVfG den Betroffenen ein **Akteneinsichtsrecht**. § 72 Abs. 5 HSchulG präzisiert dieses allgemeine Verfahrensrecht. § 72 Abs. 5 HSchulG ist auf Fälle anzuwenden, in denen Eltern, Schülerinnen und Schüler auch außerhalb eines Verwaltungsverfahrens Unterlagen, die Daten über sie enthalten, einsehen wollen.

Dem HDSG ließe sich zwar für diese Fälle ebenfalls ein Akteneinsichtsrecht entnehmen (§ 18 Abs. 4), die Vorschrift ist allerdings nicht so eindeutig formuliert. Deswegen ist streitig, ob die Behörde nicht eine Wahlmöglichkeit zwischen der Gewährung der Akteneinsicht und der Erteilung einer Auskunft hat. Das Schulgesetz trifft hier eine klare Regelung im Sinne eines umfassenden Informationsanspruches: Eltern, Schülerinnen und Schüler haben das Recht, Akten der Schule, der Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Dieses Recht können auch Schülerinnen und Schüler unter 18 Jahren ausüben.

Das Gesetz macht für die Schulen, für alle Beteiligten rechtsverbindlich, was bereits die Richtlinien des Hessischen Kultusministeriums über die Führung, Aufbewahrung und Archivierung von Schriftgut in Schulen vom 1. März 2007 (ABl. 2007 S. 223) eröffneten. Ziff. A III Nr. 4 gewährt den Erziehungsberechtigten und Schülern der Jahrgangsstufen 10 bis 13 schon seit Jahren die Möglichkeit zur Akteneinsicht. Neu ist freilich die Ausdehnung des Einsichtsrechts auf die Unterlagen der Schulaufsichtsbehörden und

des schulärztlichen Dienstes. Neu ist außerdem, und das ist das Bedeutsame an der Vorschrift, die fast vorbehaltlose gesetzliche Anerkennung eines Akteneinsichtsrechts. Lediglich wenn die Daten der Betroffenen mit Angaben Dritter derart verbunden sind, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, ist die Einsichtnahme unzulässig. In diesem Fall ist die Behörde zur Auskunft verpflichtet.

Gänzlich neu ist die Vorschrift des § 72 Abs. 4 HSchulG.
Ihre Entstehung verdankt sie den Geschehnissen im Zusammenhang mit dem Massaker an einer Schule in Erfurt in den vergangenen Jahren. Fatal hatte sich dort der Umstand ausgewirkt, dass die Eltern des volljährigen Täters über dessen schulische Entwicklungen nicht im Bilde waren und deshalb in die Kausalkette nicht eingreifen konnten. Verschiedene Bundesländer haben daher inzwischen gesetzliche Regelungen geschaffen, um eine Information auch an die Eltern volljähriger Schüler und Schülerinnen zu ermöglichen und damit einer Entwicklung wie in Erfurt frühzeitig entgegenzuwirken.

Hessen hat allerdings, wie einige Bundesländer auch, dabei das zunächst nicht einschränkbare informationelle Selbstbestimmungsunrecht des volljährigen Schülers in angemessener Weise gewichtet. Zum einen dürfen Gegenstand der Übermittlung nur „wesentliche, das Schulverhältnis betreffende Sachverhalte, insbesondere über Versetzungsgefährdungen und Nichtversetzung sowie über Ordnungsmaßnahmen nach § 82 Abs. 2 Nr. 5 bis 8 und Abs. 8“ sein. Dies schließt die Übermittlung von Informationen über unwesentliche Sachverhalte im Schulalltag aus. Die Abgrenzung hat sich am Grundsatz der Verhältnismäßigkeit zu orientieren. Auch ist dem Schüler oder der Schülerin ein spezielles Widerspruchsrecht für den besonderen Fall einer solchen Datenübermittlung an die Eltern zugebilligt. Daraus folgt, dass die Schule den Betroffenen im Einzelfall zunächst über die Absicht der Übermittlung informieren muss. Allerdings darf die Schule über den Widerspruch wiederum die Eltern informieren. Dies ist im Hinblick auf die einschlägige Rechtsprechung zur datenschutzrechtlichen Position eines volljährigen Schülers hinnehmbar.

9. Minderjährige Schülerinnen und Schüler

Ist die Datenverarbeitung nur mit Einwilligung der Betroffenen zulässig, stellt sich in der Schule zwangsläufig die Frage, ob auch minderjährige Schülerinnen und Schüler wirksam einwilligen können. Für die Datenverarbeitung zu Forschungszwecken hat der Gesetzgeber dies verneint und die **Einwilligung der Erziehungsberechtigten** verlangt (vgl. § 84 Abs. 2 HSchulG).

Im Übrigen gilt, dass auch minderjährige Schülerinnen und Schüler eine wirksame Einwilligungserklärung abgeben können. Nach allgemeiner Ansicht kommt es nicht auf die Geschäftsfähigkeit an, sondern darauf, ob Schülerinnen und Schüler psychisch und intellektuell in der Lage sind, die Tragweite der Entscheidung abzuschätzen. Fehlt die **Einsichtsfähigkeit**, bedarf es zwingend der Einwilligung der Erziehungsberechtigten. Ist Einsichtsfähigkeit gegeben, kann die Einwilligung von Schülerinnen und Schülern

nicht durch eine Erklärung der Erziehungsberechtigten ersetzt werden.

Der verständliche Wunsch der Schulen nach einer Faustformel für die Entscheidung, in welchen Fällen die Einwilligung der Schülerinnen und Schüler oder der Erziehungsberechtigten eingeholt werden muss, lässt sich nicht erfüllen. Altersregelungen in anderen Gesetzen bieten lediglich Anhaltspunkte. So kann ein Kind nach Vollendung des 14. Lebensjahres sich entscheiden, zu welcher Religion es sich bekennen will. Im Ehescheidungsverfahren darf ein 14-jähriges Kind vorschlagen, welchem Elternteil das Gericht die elterliche Sorge zusprechen soll. Ein Fünfzehnjähriger kann Sozialleistungen beantragen und entgegennehmen. Die meisten Schülerinnen und Schüler im Alter von 14 bis 15 Jahren dürften daher auch in der Lage sein, die Folgen der Verwendung ihrer Daten beurteilen zu können. Je jünger die Schülerinnen und Schüler sind, desto höhere Sorgfalt ist bei der Vorabinformation über Zweck und Umfang der Datenverarbeitung, über Löschung, Widerspruchs- und Auskunftsrecht notwendig.

§ 72 Abs. 4 HSchulG gibt nicht nur den Erziehungsberechtigten und volljährigen Schülerinnen und Schülern, sondern auch „Jugendlichen“ das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Da das Gesetz nicht festlegt, ab welchem Alter ein Schüler als Jugendlicher gilt, ist auch hier jeweils eine Einzelfallentscheidung nötig. Dabei kann § 1 Abs. 2 Jugendgerichtsgesetz als Faustformel herangezogen werden. Danach ist Jugendlicher, wer das 14. Lebensjahr vollendet hat. Wie im Fall der Einwilligung kommt es jeweils auf die tatsächliche Einsichtsfähigkeit des Schülers in Bezug auf den Verantwortungszweck an.

10. Schulgesundheitspflege und schulpsychologischer Dienst

§ 71 HSchulG

(1) Soweit zur Vorbereitung einer Entscheidung nach diesem Gesetz schulärztliche oder schulpsychologische Untersuchungen sowie sonderpädagogische Überprüfungen erforderlich werden, sind die Kinder, Jugendlichen und volljährigen Schülerinnen und Schüler verpflichtet, sich untersuchen zu lassen und an wissenschaftlich anerkannten Testverfahren teilzunehmen.

(2) Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler haben die für die Untersuchungen erforderlichen Angaben zu machen. Kinder, Jugendliche und volljährige Schülerinnen und Schüler dürfen dabei in der Regel nicht befragt werden über Angelegenheiten, die ihre oder die Persönlichkeitssphäre ihrer Eltern oder Angehörigen betreffen.

(3) Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler sind über die Untersuchungen und Testverfahren vorher näher zu informieren. Ihnen ist Gelegenheit zur Besprechung der Ergebnisse und zur Einsicht in die Unterlagen zu geben.

(4) Für Untersuchungen im Rahmen der Schulgesundheitspflege gelten Abs. 1 bis 3 entsprechend. Dabei können auch röntgenologische Untersuchungen sowie percutane und intracutane Tuberkuloseproben angeordnet werden.

(5) Die nähere Ausgestaltung der Schulgesundheitspflege und die Zulassung der für sie erforderlichen Untersuchungen erfolgt durch Rechtsverordnung.

(6) Diese Vorschriften gelten auch für die Schulen in freier Trägerschaft.

§ 83 Abs. 6 HSchulG

Im Rahmen der Schulgesundheitspflege und des schulpsychologischen Dienstes dürfen die für die Durchführung der schulärztlichen oder schulpsychologischen Untersuchungen sowie sonderpädagogischen Überprüfungen nach § 71 erforderlichen personenbezogenen Daten verarbeitet werden. Der schulärztliche und der schulpsychologische Dienst dürfen der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln. Personenbezogene Daten über freiwillige Untersuchungen dürfen nur mit schriftlicher Einwilligung der Betroffenen übermittelt werden. Medizinische Befunde dürfen nicht automatisiert verarbeitet werden, ausgenommen die medizinischen Befunde der für die Schulgesundheitspflege zuständigen Behörden (§ 149). Personenbezogene Daten des schulpsychologischen Dienstes dürfen nur automatisiert verarbeitet werden, wenn sie dabei nach dem jeweiligen Stand der Technik hinreichend sicher verschlüsselt werden.

Mit diesen Vorschriften hat der Gesetzgeber **erstmals ausreichende Rechtsgrundlagen** für die Datenverarbeitung der Schulärzte, Schulzahnärzte und des schulpsychologischen Dienstes geschaffen. Das durch das Schulgesetz abgelöste Schulverwaltungsgesetz und das Schulpflichtgesetz enthielten lediglich eine allgemeine Duldungs- und Auskunftspflicht der Schülerinnen und Schüler und Erziehungsberechtigten. Dass diese Regelung angesichts der Sensibilität der Daten, die diese Stellen verarbeiten, nicht der vom Bundesverfassungsgericht geforderten gesetzlichen Verarbeitungsbefugnis entsprach, war daher völlig klar.

Konkretisiert wurden die Einzelheiten zur Schulgesundheitspflege durch die in § 71 Abs. 5 erwähnte Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege vom 7. Februar 2000 (StAnz. 2000, S. 752). Schulärztliche Untersuchungen erfolgen beispielsweise bei der Einschulung und mindestens zwei weitere Male im Laufe der Schulzeit, außerdem in besonderen Fällen, etwa bei auftretenden Hör- und Sprachstörungen einer Schülerin und eines Schülers oder vor der Überweisung in eine Sonderschule. Schulzahnärztliche Untersuchungen werden einmal jährlich durchgeführt. Von dem bei den staatlichen Schulämtern, den unteren Schulaufsichtsbehörden, eingerichteten schulpsychologischen Dienst werden Schülerinnen und Schüler vor einer Entscheidung über die Zurückstellung von der Teilnahme am Unterricht der Grundschule oder vor

einer Überweisung in eine Sonderschule untersucht und einem wissenschaftlich anerkannten Testverfahren unterzogen.

§ 71 Abs. 2 enthält eine wichtige **Beschränkung** für derartige Untersuchungen. Kinder, Jugendliche und auch volljährige Schülerinnen und Schüler dürfen bei schulärztlichen und schulpsychologischen Pflichtuntersuchungen „in der Regel“ über Angelegenheiten, die ihre oder die Persönlichkeitssphäre der Eltern und Angehörigen betreffen, nicht befragt werden. Der Gesetzentwurf wollte solche Fragen sogar ausnahmslos verbieten, was manche notwendige Untersuchung verhindert oder zumindest unangemessen erschwert hätte. Denn es gibt durchaus Fälle, in denen es sinnvoller ist, die Schülerinnen und Schüler statt die Erziehungsberechtigten zu befragen. Das gilt besonders bei Kindesmisshandlungen oder sexuellem Missbrauch in der Familie.

Für **Transparenz** sorgt § 71 Abs. 3. Die Erziehungsberechtigten der betroffenen Schülerinnen und Schüler müssen vorher über die Untersuchungen und Testverfahren aufgeklärt werden. Darüber hinaus sind auch die „jugendlichen“ und die volljährigen Schülerinnen und Schüler zu informieren. Erziehungsberechtigte, Jugendliche und volljährige Schülerinnen und Schüler haben außerdem das Recht, die über die Untersuchungen und Tests angefertigten Unterlagen der Schulärzte und Schulpsychologen einzusehen. Beschränkungen, wie sie die ältere Rechtsprechung für die Einsicht der Patientinnen und Patienten in medizinische Unterlagen entwickelt hatte, sind hier nicht vorgesehen.

§ 83 Abs. 6 stellt sicher, dass die Schulen und Aufsichtsbehörden nur diejenigen Untersuchungsdaten erheben und weiterverarbeiten, die sie für ihre schulverwaltungsfachlichen und pädagogischen Entscheidungen benötigen. Im Gesetzgebungsverfahren bestand Einvernehmen, dass die Mitteilung des **Untersuchungsergebnisses** genügt. Deshalb schreibt das Gesetz vor, dass der schulärztliche und der schulpsychologische Dienst der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln dürfen.

Schulpsychologen werden nicht nur im Rahmen von Pflichtuntersuchungen tätig, sondern auch auf Wunsch von Erziehungsberechtigten, Schülerinnen und Schülern oder auf Anraten von Lehrern. Diese freiwilligen Untersuchungen sind zu behandeln wie Konsultationen frei praktizierender Psychologen. Das Gesetz schreibt die früher im Erlass des Hessischen Kultusministeriums dazu vorgesehene Regelung fest: Informationen über freiwillige Untersuchungen und Beratungen dürfen nur mit schriftlicher Einwilligung der Betroffenen weitergegeben werden. Automatisierte Verarbeitungen sind insofern unzulässig.

Die Einbeziehung der Datenverarbeitung im Rahmen der Schulgesundheitspflege und die Offenbarungs- und Mitwirkungspflichten der Eltern, Schülerinnen und Schüler in § 71 Abs. 4 waren notwendig, um eine möglichst umfassende Durchführung sicherzustellen.

11. Datensicherheit

§ 83 Abs. 7 HSchulG

Die automatisierte Verarbeitung personenbezogener Daten darf in der Schule nur mit schuleigenen Datenverarbeitungsgeräten erfolgen, es sei denn, dass die Beachtung der erforderlichen Datensicherheitsmaßnahmen gewährleistet ist.

In der Vorläuferfassung, dem § 83 Abs. 5 HSchulG, war ein generelles Verbot enthalten, die automatisierte Datenverarbeitung in der Schule mit DV-Geräten zu betreiben, die nicht im Eigentum der Schule standen. Dies hing mit der wegen des Eigentums Dritter eingeschränkten Kontrollierbarkeit der Geräte zusammen, insbesondere durch den schulischen Datenschutzbeauftragten, soweit das Gerät Schulverwaltungsdaten enthält. Die Nutzung vor allem von mobilen DV-Geräten der Lehrkräfte (Laptops, Handhelds, Palms, Handys) in der Schule zu Schulverwaltungszwecken nimmt aber permanent zu, weshalb ein generelles Verbot der Nutzung privater DV-Geräte lebensfremd wäre. Voraussetzung einer solchen Nutzung ist allerdings ausdrücklich die Gewährleistung der Datensicherheit nach § 10 HDSG. Deshalb hat die Schulleitung den Einsatz einer solchen Nutzung kraft der Dienstaufsicht zu verbieten, wenn die Datensicherheit nicht gesichert ist. Dazu muss die Lehrkraft auf Befragen Angaben machen.

12. Lehrerdaten

§ 83 HSchulG

(1) Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, soweit die Kenntnis der Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist.

(2) Schulträger und Schulaufsichtsbehörden dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben der Schulplanung, der Schulorganisation und der Schulaufsicht und einem jeweils damit verbundenen Zweck oder zur Durchführung organisatorischer Maßnahmen erforderlich ist. Abs. 1 Satz 2 gilt entsprechend.

(3) ... Lehrerinnen und Lehrer sind verpflichtet, die erforderlichen Angaben zu machen.

(4) Zur Evaluation der Schulen nach § 98 können die Schulen und die Schulaufsichtsbehörden oder von ihnen beauftragte Dritte methodisch geeignete Verfahren einsetzen und durch Befragungen, Erhebungen und

Unterrichtsbeobachtungen gewonnene Daten verarbeiten. Die Betroffenen werden vorab über das Ziel des Vorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung ihrer Daten sowie über die zur Einsichtnahme in die Daten und Ergebnisse Berechtigten informiert. Personenbezogene Daten für diese Zwecke dürfen ohne Einwilligung der Betroffenen verarbeitet werden, wenn das öffentliche Interesse an der Durchführung eines von der obersten Schulaufsichtsbehörde veranlassten oder genehmigten Vorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann. Unter diesen Voraussetzungen dürfen personenbezogene Daten auch Dritten, die mit der externen Evaluation beauftragt sind, überlassen werden. § 33 Abs. 2 und 3 des Hessischen Datenschutzgesetzes gilt entsprechend.

§ 50 BeamtStG

Für jede Beamtin und jeden Beamten ist eine Personalakte zu führen. Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Die Personalakte ist vertraulich zu behandeln. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein. Für Ausnahmefälle kann landesrechtlich eine von Satz 4 abweichende Verwendung vorgesehen werden.

§ 107 HBG

(1) Über jeden Beamten ist eine Personalakte zu führen; sie ist vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Zur Personalakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. Personalakten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein. Nicht Bestandteil der Personalakte sind Unterlagen, die besonderen, von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, insbesondere Prüfungs-, Sicherheits- und Kindergeldakten. Kindergeldakten können mit Besoldungs- und Versorgungsakten verbunden geführt werden, wenn diese von der übrigen Personalakte getrennt sind und von einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden; § 35 des Ersten Buches Sozialgesetzbuch und die §§ 67 bis 78 des Zehnten Buches Sozialgesetzbuch bleiben unberührt.

(2) Die Personalakte kann nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert werden. Teilakten können bei der für den betreffenden Aufgabenbereich

zuständigen Behörde geführt werden. Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur geführt werden, wenn die Personal verwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere Personal verwaltende Behörden für den Beamten zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. In die Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen.

(3) Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

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

§ 107a HBG

(1) Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Bei automatisierter Beihilfebearbeitung (§ 107g Abs. 2) ist ausnahmsweise die Zusammenfassung der Beihilfebescheide in Sachakten zulässig, sofern der Datenschutz gesichert und gewährleistet ist, dass die Beihilfe-Teilakte jederzeit wieder zusammengeführt werden kann.

(2) Die Beihilfeakten und Beihilfedaten dürfen für andere als für Beihilfezwecke nur verwendet oder weitergegeben werden, wenn der Beihilfeberechtigte und der bei der Beihilfegewährung berücksichtigte Angehörige im Einzelfall einwilligen, die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

(3) Abs. 1 und 2 gelten entsprechend für Unterlagen über Heilfürsorge und Heilverfahren.

§ 107b HBG

Der Beamte ist zu Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder ihm nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören, soweit die Anhörung nicht nach anderen Rechtsvorschriften erfolgt. Die Äußerung es Beamten ist zur Personalakte zu nehmen.

§ 107c HBG

(1) Der Beamte hat, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständige Personalakte.

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

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

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

§ 107d HBG

(1) Ohne Einwilligung des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das Gleiche gilt für Behörden desselben Geschäftsbereichs, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist, sowie für Behörden eines anderen Geschäftsbereichs desselben Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken haben. Ärzten, die im Auftrag der Personal verwaltenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden. Für Auskünfte aus der Personalakte gelten Satz 1 bis 3 entsprechend. Soweit eine Auskunft ausreicht, ist von einer Vorlage

abzusehen.

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

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

§ 107e HBG

(1) Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendung finden, sind

1. *falls sie sich als unbegründet oder falsch erwiesen haben, mit Zustimmung des Beamten unverzüglich aus der Personalakte zu entfernen und zu vernichten,*
2. *falls sie für den Beamten ungünstig sind oder ihm nachteilig werden können, auf Antrag des Beamten nach drei Jahren zu entfernen und zu vernichten; dies gilt nicht für dienstliche Beurteilungen.*

Die Frist nach Satz 1 Nr. 2 wird durch erneute Sachverhalte im Sinne dieser Vorschrift oder durch die Einleitung eines Straf- oder Disziplinarverfahrens unterbrochen. Stellt sich der erneute Vorwurf als unbegründet oder falsch heraus, gilt die Frist als nicht unterbrochen.

(2) Mitteilungen in Strafsachen, soweit sie nicht Bestandteil einer Disziplinarakte sind, sowie Auskünfte aus dem Bundeszentralregister sind mit Zustimmung des Beamten nach drei Jahren zu entfernen und zu vernichten. Abs. 1 Satz 2 und 3 gilt entsprechend.

§ 107f HBG

(1) Personalakten sind nach ihrem Abschluss von der Personalakten führenden Behörde fünf Jahre aufzubewahren. Personalakten sind abgeschlossen,

1. *wenn der Beamte ohne Versorgungsansprüche aus dem öffentlichen Dienst ausgeschieden ist, mit Ablauf des Jahres der Vollendung des fünfundsechzigsten Lebensjahres, in den Fällen des § 48 dieses Gesetzes und des § 9 der Hessischen Disziplinarordnung jedoch erst, wenn mögliche Versorgungsempfänger nicht mehr vorhanden sind,*
2. *wenn der Beamte ohne versorgungsberechtigte Hinterbliebene verstorben ist, mit Ablauf des Todesjahres,*
3. *wenn nach dem verstorbenen Beamten versorgungsberechtigte Hinterbliebene vorhanden sind, mit Ablauf des Jahres, in dem die letzte Versorgungspflicht entfallen ist.*

(2) Unterlagen über Beihilfe, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sind drei Jahre und über Umzugs- und Reisekosten

sechs Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden.

(3) Versorgungsakten sind fünf Jahre nach Ablauf des Jahres, in dem die letzte Versorgungszahlung geleistet worden ist, aufzubewahren; besteht die Möglichkeit eines Wiederauflebens des Anspruchs, sind die Akten dreißig Jahre aufzubewahren.

(4) Die Personalakten werden nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen Staatsarchiv übernommen werden.

§ 107g HBG

(1) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden. Ihre Übermittlung ist nur nach Maßgabe des § 107d zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

(2) Personalaktendaten im Sinne des § 107a dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.

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

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

(5) Bei erstmaliger Speicherung ist dem Betroffenen die Art der über ihn nach Abs. 1 gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er zu benachrichtigen. Ferner sind die Verarbeitungs- und Nutzungsformen automatisierter Personalverwaltungsverfahren zu dokumentieren und einschließlich des jeweiligen Verwendungszwecks sowie der regelmäßigen Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekannt zu geben.

§ 1 Abs. 8 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009:

Schulen dürfen
– für die Planung und Durchführung der Unterrichtsorganisation

– für die Fortschreibung der amtlichen Schuldaten
die in Anlage 1 Abschnitt B enthaltenen Personalstammdaten der Lehrerinnen und Lehrer verarbeiten. Dies schließt die Verarbeitung weiterer, lediglich schulorganisatorischer Daten nicht aus. Im Übrigen gelten die Regelungen des § 34 HDSG.

§ 34 HDSG

(1) Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(3) Das Auskunftsrecht nach § 18 Abs. 3 umfasst auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 6 findet keine Anwendung.

(4) Im Falle des § 19 Abs. 3 Satz 1 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Vor Einführung, Anwendung, Änderung oder Erweiterung eines automatisierten Verfahrens zur Verarbeitung von Daten der Beschäftigten hat die Dienststelle das Verfahrensverzeichnis (§ 6) der Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens mit dem Hinweis vorzulegen, dass sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann. Macht die Personalvertretung von dieser Möglichkeit Gebrauch, beginnt die von ihr einzuhaltende Frist erst mit der Vorlage der von der Dienststellenleitung einzuholenden Stellungnahme.

(6) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

Die Verarbeitung personenbezogener Daten des Lehrpersonals ist in zweifacher Hinsicht gegenüber § 34 HDSG speziell geregelt, der generell für die Bediensteten in der hessischen Landes- und Kommunalverwaltung gilt und sozusagen die „ Arbeitnehmerdatenschutznorm“ für den öffentlichen Dienst in Hessen darstellt.

In personeller Hinsicht gibt es eine Spezialvorschrift im Schulgesetz (§ 83), in sachlicher Hinsicht im Beamtengesetz, nämlich das Personalaktenrecht (§§ 107 ff. HBG, § 50 BeamtStG).

Da die Personalverwaltung der Lehrer grundsätzlich durch das jeweils zuständige Staatliche Schulamt erfolgt, benötigen die Schulen nur in relativ geringem Umfang personenbezogene Lehrerdaten in den dortigen Teilakten, soweit es die Aufgaben des Schulleiters als Dienstvorgesetzten betrifft. Das informationelle Selbstbestimmungsrecht des Lehrpersonals ist zu Gunsten der - verallgemeinert formuliert - „Funktionsfähigkeit“ des Schulwesens eingeschränkt. Dabei reicht es für die Zulässigkeit der Verarbeitung personenbezogener Daten des Lehrpersonals nicht aus, dass die Datenverarbeitung für die Sicherung des Schulbetriebs nur nützlich ist; notwendig ist die Erforderlichkeit der Datenverarbeitung für die jeweils verfolgten schulischen Zwecke. Mit der Verarbeitungsbefugnis der staatlichen Schulverwaltung korrespondiert eine entsprechende Pflicht der Lehrerinnen und Lehrer, die insoweit erforderlichen Auskünfte zu geben. Wichtigstes Dokument für die personenbezogenen Daten der Lehrerinnen und Lehrer ist die jeweilige Personalakte, die von den staatlichen Schulämtern verwaltet wird.

Die in der Schule verwahrten Personalteilakten der Lehrkräfte unterliegen dem besonderen Zugriffsschutz gemäß § 107 Abs. 1 HBG und § 50 BeamtStG. Eine persönliche Zugriffskontrolle hinsichtlich jeder einzelnen Akte und eine besonders sichere Aufbewahrung in abgeschlossenen Aktenschränken, am besten im Zimmer der Schulleitung, sind hier unverzichtbar.

Durch die letzte Änderung des Schulgesetzes gänzlich neu und deshalb hervorzuheben sind die Abs. 4 und 5 des § 83. Sie beschäftigen sich mit der **Evaluation** des Unterrichts. Die Einführung der Evaluation in dem Spektrum öffentlicher Dienstleistungen – dazu gehört auch die Schule – kann insofern schon auf eine gewisse Entwicklung zurückschauen, als sie nach den gesetzlichen Vorgaben des Hessischen Hochschulgesetzes in den Hessischen Hochschulen seit langem und nun verstärkt zur Verbesserung der Lehre eingesetzt wird. Beim Einsatz der unterschiedlichen Instrumentarien der Evaluation können auch personenbezogene Daten der Dozentinnen und Dozenten verarbeitet werden, so etwa durch Befragung der Studierenden über die Qualität der Vorlesungen. Zu den hierbei entstandenen datenschutzrechtlichen Fragen habe ich mich vor allem in den Tätigkeitsberichten geäußert. Grundlage war dabei eine auch vom Hochschulgesetz vorgesehene, zwingend erforderliche Satzung der einzelnen Hochschulen, in der alle Details der Evaluation festzuschreiben sind. Hierzu wurde eine Mustersatzung entworfen, die auch personalrechtlichen Anforderungen standhält.

§ 83 Abs. 4 geht davon aus, dass im Rahmen einer internen oder externen Evaluierung des Unterrichts auch personenbezogene Daten der Lehrkräfte verarbeitet werden dürfen, insbesondere im Rahmen der Unterrichtsbeobachtung. Insofern bietet diese

Vorschrift eine – wenn auch noch nicht detaillierte – erste Rechtsgrundlage für diesen Kontext.

Satz 2 verlangt allerdings ausdrücklich eine umfassende vorherige Aufklärung der betroffenen Lehrkräfte über die Details der Datenverarbeitung in Anlehnung an den § 12 Abs. 4 HDSG.

Satz 3 erlaubt ausdrücklich die weitere Verarbeitung der durch die Unterrichtsbeachtung gewonnenen und sonstigen in der Schule recherchierten Daten der Lehrkräfte auch ohne deren Einwilligung unter den dann benannten Vorraussetzungen. Diese sind den Vorgaben des § 33 Abs. 1 HDSG entlehnt. Des Weiteren hat der Gesetzgeber die entsprechende Geltung der § 33 Abs. 2 und 3 HDSG ausdrücklich mit einbezogen. Damit ist auch die strenge Zweckbindung gewahrt.

Die generalklauselartigen Vorgaben des § 83 Abs. 4 erfordern jedoch wegen der teils weitreichenden Konsequenzen der Ergebnisse der Evaluierung für die betroffene Lehrkraft eine weitere normative Konkretisierung, wie sie in den o. g. Hochschulsatzungen schon vorhanden ist. Diese auf diese Weise vorzunehmenden Festlegungen können im Rahmen der in § 83 Abs. 9 vorgesehenen Rechtsverordnung erfolgen, deren Anpassung an die Änderungen des Schulgesetzes zu erwarten ist.

§ 83 Abs. 5 sieht für die weitergehenden Zwecke der Lehreraus- und -fortbildung – neben der Evaluation – die Bild- und Tonaufzeichnung des Unterrichts vor, die – neben die davon betroffenen Schüler – auch die Lehrkräfte erfasst. Die Persönlichkeitsrechte beider Personengruppen, dies nicht dulden zu müssen, sind aber ausreichend gewahrt durch die ausdrücklich vorgesehene Möglichkeit des auch mündlich möglichen Widerspruchs nach einer umfassenden Aufklärung über die vorgesehene Aufzeichnung. Wichtig ist hier vor allem die eindeutige Freiwilligkeit in der Entscheidung über den Widerspruch, gerade bei den betroffenen Schülern. Die Lehrkräfte haben sicherzustellen, dass der Klassenverband dabei ohne Einfluss bleiben muss.

13. Schulinterner Datenschutzbeauftragter

Ausführlich widmet sich die neue Verordnung dem schulischen Datenschutzbeauftragten in § 11. Sie übernimmt in Absatz 1 – wiederholend – die schon in § 5 Abs. 1 Satz 1 HDSG enthaltene Pflicht der Schule, einen Datenschutzbeauftragten sowie einen Vertreter schriftlich zu bestellen. Ergänzend wird allerdings gefordert, dass die Bestellung „im Einverständnis mit dem Betroffenen“ erfolgen soll.

Absatz 2 der Verordnung nimmt das in § 5 Abs 1 Satz 2 HDSG enthaltene Verbot der Interessenskollision auf und verbietet die Bestellung der Schulleitung zum Datenschutzbeauftragten. Sofern kleinere Schulen wenig Spielraum für die Bestellung eines eigenen Datenschutzbeauftragten haben, ist es – in Ergänzung des § 5 Abs. 3 HDSG – möglich, dass mehrere Schulen einen gemeinsamen Datenschutzbeauftragten bestellen können, nur eine Schule darf dabei aber mehr als 10 Lehrkräfte haben.

Die vielfältigen Aufgaben des schulischen Datenschutzbeauftragten sind in den Absätzen 4 bis 6 zusammengefasst, die insoweit den § 5 Abs. 2 HDSG, ergänzen. Auf der Homepage des HDSB ist eine Liste zu finden, die diese Aufgaben weiter konkretisiert.

III. Materialien

1. Schulspezifische Vorschriften

1.1 Hessisches Schulgesetz (HSchulG) – Auszug

in der Fassung vom 14. Juni 2005 (GVBl. I S. 442),
zuletzt geändert durch Gesetz vom 14. Juli 2009 (GVBl. I S. 265)

§ 71
Verpflichtung zu besonderen Untersuchungen

(1) Soweit zur Vorbereitung einer Entscheidung nach diesem Gesetz schulärztliche oder schulpsychologische Untersuchungen sowie sonderpädagogische Überprüfungen erforderlich werden, sind die Kinder, Jugendlichen und volljährigen Schülerinnen und Schüler verpflichtet, sich untersuchen zu lassen und an wissenschaftlich anerkannten Testverfahren teilzunehmen.

(2) Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler haben die für die Untersuchungen erforderlichen Angaben zu machen. Kinder, Jugendliche und volljährige Schülerinnen und Schüler dürfen dabei in der Regel nicht befragt werden über Angelegenheiten, die ihre oder die Persönlichkeitssphäre ihrer Eltern oder Angehörigen betreffen.

(3) Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler sind über die Untersuchungen und Testverfahren vorher näher zu informieren. Ihnen ist Gelegenheit zur Besprechung der Ergebnisse und zur Einsicht in die Unterlagen zu geben.

(4) Für Untersuchungen im Rahmen der Schulgesundheitspflege gelten Abs. 1 bis 3 entsprechend. Dabei können auch röntgenologische Untersuchungen sowie percutane und intracutane Tuberkuloseproben angeordnet werden.

(5) Die nähere Ausgestaltung der Schulgesundheitspflege und die Zulassung der für sie erforderlichen Untersuchungen erfolgt durch Rechtsverordnung.

(6) Diese Vorschriften gelten auch für die Schulen in freier Trägerschaft.

§ 72
Informationsrechte der Eltern und der Schülerinnen und Schüler

(3) Die Schulleiterin oder der Schulleiter sowie die Lehrerinnen und Lehrer sollen die Eltern und Schülerinnen und Schüler in angemessenem Umfang informieren und beraten über

1. die Lernentwicklung sowie das Arbeits- und Sozialverhalten der Schülerin oder des Schülers, insbesondere bei Lern- und Verhaltensstörungen,
2. die Leistungsbewertung einschließlich der Versetzungen und Kurseinstufungen sowie
3. die Wahl der Bildungsgänge.

(4) Die Eltern volljähriger Schülerinnen und Schüler sind bis zur Vollendung des 21. Lebensjahres über wesentliche, das Schulverhältnis betreffende Sachverhalte, insbesondere über Versetzungsgefährdungen und Nichtversetzungen sowie über Ordnungsmaßnahmen nach § 82 Abs. 2 Nr. 5 bis 8 und Abs. 8 zu informieren, sofern die volljährige Schülerin oder der volljährige Schüler dem nicht widersprochen hat. Über den Widerspruch werden die Eltern von der Schule informiert. Die Schülerinnen und Schüler sind auf diese Regelung hinzuweisen.

(5) Jugendliche, die Eltern und volljährige Schülerinnen und Schüler haben das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter derart verbunden sind, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist den Betroffenen über die zu ihrer Person gespeicherten Daten Auskunft zu erteilen.

(6) Diese Vorschrift gilt auch für Schulen in freier Trägerschaft.

§ 82
Pädagogische Maßnahmen und Ordnungsmaßnahmen

(10) Eintragungen und Vorgänge über Ordnungsmaßnahmen sind spätestens am Ende des zweiten Schuljahres nach der Eintragung zu löschen, sofern nicht während dieser Zeit eine erneute Ordnungsmaßnahme getroffen wurde.

§ 83
Erhebung und Verarbeitung von personenbezogenen Daten

(1) Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, soweit die Kenntnis der Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist.

(2) Schulträger und Schulaufsichtsbehörden dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben

der Schulplanung, der Schulorganisation und der Schulaufsicht und einem jeweils damit verbundenen Zweck oder zur Durchführung organisatorischer Maßnahmen erforderlich ist. Abs. 1 Satz 2 gilt entsprechend.

(3) Schülerinnen und Schüler, deren Eltern und Lehrerinnen und Lehrer sind verpflichtet, die erforderlichen Angaben zu machen.

(4) Zur Evaluation der Schulen nach § 98 können die Schulen und die Schulaufsichtsbehörden oder von ihnen beauftragte Dritte methodisch geeignete Verfahren einsetzen und durch Befragungen, Erhebungen und Unterrichtsbeobachtungen gewonnene Daten verarbeiten. Die Betroffenen werden vorab über das Ziel des Vorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung ihrer Daten sowie über die Einsichtnahme in die Daten und Ergebnisse Berechtigten informiert. Personenbezogene Daten für diese Zwecke dürfen ohne Einwilligung der Betroffenen verarbeitet werden, wenn das öffentliche Interesse an der Durchführung eines von der obersten Schulaufsichtsbehörde veranlassten oder genehmigten Vorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann. Unter diesen Voraussetzungen dürfen personenbezogene Daten auch Dritten, die mit der externen Evaluation beauftragt sind, überlassen werden. § 33 Abs. 2 und 3 des Hessischen Datenschutzgesetzes gilt entsprechend.

(5) Für Zwecke der Lehreraus- und -fortbildung sowie der Qualitätsentwicklung des Unterrichts dürfen Bild- und Tonaufzeichnungen des Unterrichts erfolgen, wenn die Betroffenen rechtzeitig über die beabsichtigte Aufzeichnung und den Aufzeichnungszweck schriftlich informiert worden sind und nicht widersprochen haben. Die Aufzeichnungen sind spätestens nach fünf Jahren zu löschen, soweit schutzwürdige Belange der Betroffenen nicht eine frühere Löschung erfordern.

(6) Im Rahmen der Schulgesundheitspflege und des schulpsychologischen Dienstes dürfen die für die Durchführung der schulärztlichen oder schulpsychologischen Untersuchungen sowie sonderpädagogischen Überprüfungen nach § 71 erforderlichen personenbezogenen Daten verarbeitet werden. Der schulärztliche und der schulpsychologische Dienst dürfen der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln. Personenbezogene Daten über freiwillige Untersuchungen dürfen nur mit schriftlicher Einwilligung der Betroffenen übermittelt werden. Medizinische Befunde dürfen nicht automatisiert verarbeitet werden, ausgenommen die medizinischen Befunde der für die Schulgesundheitspflege zuständigen Behörden (§ 149). Personenbezogene Daten des schulpsychologischen Dienstes dürfen nur automatisiert verarbeitet werden, wenn sie dabei nach dem jeweiligen Stand der Technik hinreichend sicher verschlüsselt werden.

(7) Die automatisierte Verarbeitung personenbezogener Daten darf in der Schule nur mit schuleigenen Datenverarbeitungsgeräten erfolgen, es sei denn, dass die Beachtung der erforderlichen Datensicherheitsmaßnahmen gewährleistet ist.

(8) Soweit in diesem Gesetz nichts anderes geregelt ist, gilt das Hessische Datenschutzgesetz in der jeweils geltenden Fassung.

(9) Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule werden durch Rechtsverordnung näher geregelt; dabei ist zu bestimmen, welche Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten außerhalb der Schule zu berücksichtigen sind.

§ 84
Wissenschaftliche Forschung

(1) Wissenschaftliche Forschungsvorhaben in Schulen bedürfen der Genehmigung des Kultusministeriums; die Befugnis kann auf die Schulaufsichtsbehörden übertragen werden. Die Genehmigung erziehungswissenschaftlicher Forschungsvorhaben soll erteilt werden, wenn die Erfüllung des Bildungsauftrages der Schule hierdurch nicht unangemessen beeinträchtigt wird. Vor Erteilung der Zustimmung ist die Schulkonferenz zu hören. Die Genehmigung von Forschungsvorhaben, bei denen personenbezogene Daten verarbeitet werden, ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Personenbezogene Daten dürfen für ein bestimmtes wissenschaftliches Forschungsvorhaben in der Regel nur mit Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler verarbeitet werden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Personenbezogene Daten dürfen ohne Einwilligung der Betroffenen verarbeitet werden, soweit deren schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung der Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung ohne Rechtsnachteile verweigern können; sie sind dabei über das Ziel und den wesentlichen Inhalt des Forschungsvorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung der erhobenen Daten aufzuklären. § 33 Abs. 2 und 3 des Hessischen Datenschutzgesetzes gilt entsprechend.

(3) Abs. 2 gilt entsprechend für Untersuchungen in Schulen, die vom Kultusministerium oder in dessen Auftrag durchgeführt werden.

§ 85
Statistische Erhebungen

Durch Rechtsverordnung können die öffentlichen Schulen und im Rahmen der in Art. 7 Abs. 4 des Grundgesetzes gewährten Privatschulfreiheit die Träger von Schulen in freier Trägerschaft verpflichtet werden, für statistische Zwecke Daten über schul- und

ausbildungsbezogene Tatbestände zur Evaluierung, Bildungsberichterstattung und Bildungsplanung an das Kultusministerium und an das Statistische Landesamt zu übermitteln. Das Statistische Landesamt kann Einzelangaben für die in Satz 1 genannten Zwecke auf Anforderung auch dem Kultusministerium übermitteln, wenn beim Empfänger die statistische Geheimhaltung durch personelle, organisatorische und räumliche Abschottung gewährleistet ist. Im Übrigen findet das Hessische Landesstatistikgesetz vom 19. Mai 1987 (GVBl. I S. 67, zuletzt geändert durch Gesetz vom 11. Dezember 2007 (GVBl. I S. 921), entsprechende Anwendung.

1.2 Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen

vom 4. Februar 2009 (ABl. 2009 S. 131)

Aufgrund §§ 83 Abs. 9 und 85 in Verbindung mit § 185 Abs. 1 des Hessischen Schulgesetzes in der Fassung vom 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 14. Juli 2009 (GVBl. I S. 265) wird verordnet:

Inhaltsübersicht

ERSTER TEIL
Verarbeitung personenbezogener Daten in Schulen

§ 1
Grundsätze

(1) Schulen und Schulaufsichtsbehörden dürfen nach § 83 des Hessischen Schulgesetzes sowie nach den allgemeinen datenschutzrechtlichen Vorschriften die in der Anlage 1 dieser Verordnung genannten personenbezogenen Daten der Schülerinnen und Schüler und ihrer Eltern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck, zur Durchführung schulorganisatorischer Maßnahmen oder zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich ist.

(2) Die öffentlichen Schulen sind verpflichtet, die Lehrer- und Schülerdatenbank (LUSD) zu nutzen und die verpflichtet vorgegebenen Daten zeitnah einzugeben und zu aktualisieren. Schulen in freier Trägerschaft können die Lehrer- und Schülerdatenbank (LUSD) nutzen, wenn sie die Geltung des Hessischen Datenschutzgesetzes und dieser Verordnung anerkennen.

(3) Schulen führen Schulakten (Vorgänge der allgemeinen Verwaltung der Schule) und legen für jede Schülerin und jeden Schüler eine Schülerdatei an, in der die personenbezogenen Daten gespeichert werden. Die Schülerdatei kann in elektronischer Form (LUSD) und in Papierform (Schülerakte mit Schülerkarte) geführt werden. Die Schülerkarte kann durch den jeweils aktuellen Ausdruck des Stammdatenblatts und der Dokumentation des Bildungsgangs aus der LUSD ersetzt werden.

(4) Jede Lehrkraft ist verpflichtet, die in ihren Aufgabenbereich fallenden Daten einzutragen und die erforderlichen Nachweise zu führen.

(5) Auf privaten Datenverarbeitungseinrichtungen dürfen Lehrkräfte nach Maßgabe des § 3 personenbezogene Daten von Schülerinnen und Schülern oder Eltern nur im Zusammenhang mit eigenem Unterricht oder Klassenführung verarbeiten. Ebenso ist die Verarbeitung personenbezogener Daten zulässig, deren Verarbeitung für die Lehrkraft im Rahmen einer eigenen schulischen Funktion erforderlich ist. Darüber hinaus dürfen Förderschullehrkräfte und Berufsschullehrkräfte mit sonderpädagogischer Zusatzausbildung die zur Erstellung von sonderpädagogischen Gutachten erforderlichen personenbezogenen Daten verarbeiten.

(6) Daten über gesundheitliche Beeinträchtigungen und körperliche Behinderungen dürfen mit Ausnahme der in den Anlagen 1 A 4.1, A 4.5 und A 4.6 genannten schulartspezifischen Zusatzdaten nur mit der Einwilligung der Eltern oder der volljährigen Schülerin oder des volljährigen Schülers verarbeitet werden. Medizinische und psychologische Gutachten und sonstige Unterlagen mit besonders sensiblen Daten werden in einem verschlossenen Umschlag in die Schülerakte eingeheftet. Bei Einsichtnahme in diese Unterlagen müssen der Name der Leserin oder des Lesers, das Datum und der Grund der Einsichtnahme auf dem Umschlag mit Unterschrift versehen vermerkt werden. Der Umschlag ist nach jeder Einsichtnahme wieder zu verschließen. Sind solche Daten in elektronischen Dateien gespeichert, so ist sicherzustellen, dass die Speicherung nur auf Datenverarbeitungseinrichtungen der Schule und in verschlüsselter

Form erfolgt und der Zugangs- und Zugriffsschutz nach § 10 des Hessischen Datenschutzgesetzes beachtet wird.

(7) In die Schülerakte einschließlich der Prüfungsunterlagen können nach § 72 Abs. 5 des Hessischen Schulgesetzes die Eltern als Betroffene, die Eltern minderjähriger Schülerinnen und Schüler, Jugendliche, noch minderjährige Schülerinnen und Schüler nach Vollendung des 14. Lebensjahres neben den Eltern, volljährige Schülerinnen und Schüler, bevollmächtigte Eltern volljähriger Schülerinnen und Schüler und von den Berechtigten Bevollmächtigte Einsicht nehmen. Das Recht auf Einsichtnahme erstreckt sich nur auf Vorgänge, die ausschließlich die jeweilige Schülerin oder den jeweiligen Schüler oder die jeweiligen Eltern betreffen. Die Einsichtsrechte weiterer Dritter bestimmen sich nach dem Hessischen Datenschutzgesetz. Sind personenbezogene Daten automatisiert gespeichert, gilt entsprechend das Auskunftsrecht nach § 18 Abs. 3 des Hessischen Datenschutzgesetzes.

(8) Für die Planung und Durchführung der Unterrichtsorganisation dürfen die Schulen die in Abschnitt B der Anlage 1 zu dieser Verordnung genannten Daten der Lehrkräfte verarbeiten. Dies schließt die Verarbeitung weiterer lediglich schulorganisatorischer Daten nicht aus. Eine Überwachung des Verhaltens und der Leistung einzelner Lehrkräfte erfolgt nicht.

§ 2
Organisation der Datenverarbeitung

(1) Anlagen zur Verarbeitung personenbezogener Daten in Schulen dürfen mit Datenverarbeitungseinrichtungen für Unterrichtszwecke nur vernetzt werden, wenn eine zuverlässige Trennung der Daten gewährleistet ist. Nach § 10 Abs. 2 Satz 2 des Hessischen Datenschutzgesetzes muss jede Schule ein IT-Sicherheitskonzept erstellen.

(2) Geräte zur Verarbeitung personenbezogener Daten dürfen nur an Einrichtungen zur elektronischen Kommunikation angeschlossen werden, wenn die in dem Gerät gespeicherten personenbezogenen Daten durch geeignete Maßnahmen gegen unberechtigten Zugriff geschützt werden.

(3) Bei der Datenverarbeitung in Schulen sind die Standards der von dem Bundesamt für Sicherheit in der Informationstechnik für den IT-Grundschutz veröffentlichten Regeln einzuhalten.

§ 3
Verarbeitung schulischer Daten auf privaten Anlagen

(1) Eine automatisierte Verarbeitung personenbezogener Schüler- und Schuldaten durch Lehrkräfte auf privaten Datenverarbeitungseinrichtungen außerhalb der Schule darf nur nach einer entsprechenden schriftlichen Anzeige bei der Schulleitung erfolgen.

Die Anzeige muss enthalten:

1. Eine Beschreibung der vorgesehenen Datenarten und Einsatzzwecke,
2. eine Verpflichtung, die Datensicherheitsmaßnahmen im Sinne des § 10 des Hessischen Datenschutzgesetzes einzuhalten,
3. die Erklärung der Lehrkraft, sich der Kontrolle des Hessischen Datenschutzbeauftragten zu unterwerfen sowie die Verpflichtung, dessen Beauftragten nach vorheriger Terminvereinbarung Zugang zu der häuslichen Arbeitsstätte zu gewähren, um die vorhandenen Datensicherungsmaßnahmen und die Einhaltung der Datensicherungsmaßnahmen zu überprüfen. Die Verpflichtung muss die Zusicherung enthalten, dass mögliche Mitinhaberinnen oder Mitinhaber der Wohnung mit dieser Zugangsregelung einverstanden sind.

(2) Auf den privaten Datenverarbeitungseinrichtungen der Lehrkräfte dürfen nur die in Abschnitt A 6 der Anlage 1 genannten personenbezogenen Daten verarbeitet werden, soweit dies zu der jeweiligen dienstlichen Aufgabenerfüllung erforderlich ist. Nach Ende des Datenverarbeitungsvorgangs sind alle für die Schüler- oder die Schulaktenführung relevanten Daten unverzüglich zu diesen Akten zu nehmen.

(3) Bei einer automatisierten Texterstellung für Zeugnisse, Mitteilungen, Benachrichtigungen und ähnliche Schriftstücke sind die hierzu erforderlichen personenbezogenen Daten nach Abschluss der Aufgabe unverzüglich zu löschen. Ausschließlich zu dem in Satz 1 genannten Zweck ist auch die Verarbeitung von Leistungs- und Verhaltensbewertungen zulässig, die andere Lehrkräfte getroffen haben.

(4) Bei der Verarbeitung personenbezogener Daten im Rahmen der Erstellung von sonderpädagogischen Gutachten sind besondere Maßnahmen zu treffen, um diese Daten gegen unberechtigten Zugriff zu schützen. Nach Erstellung der Gutachten sind diese auf Datenverarbeitungseinrichtungen der Schule auszudrucken und alle personenbezogenen Daten unverzüglich zu löschen.

(5) Bei der Verarbeitung der personenbezogenen Daten durch eine Lehrkraft bleibt die Schule die datenverarbeitende Stelle im Sinne des Hessischen Datenschutzgesetzes und damit auch für die Datensicherheit verantwortlich.

(6) Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungseinrichtungen kann einer Lehrkraft durch die Schulleiterin oder den Schulleiter untersagt werden, wenn ein Verstoß der Lehrkraft gegen eine Bestimmung dieser Verordnung oder des Hessischen Datenschutzgesetzes festgestellt wird.

§ 4
Klassenbücher und Kurshefte

In Klassenbüchern oder Kursheften dürfen die in Abschnitt A 5 der Anlage 1 genannten Daten erfasst werden. Der Schulbesuch von Schülerinnen und Schülern aus beruflich reisenden Familien ist in einem durch die Stamm- und Stützpunktschulen zu führenden Schultagebuch zu dokumentieren. Näheres wird durch Erlass geregelt.

§ 5
Allgemeine Bestimmungen für die Übermittlung von Daten

Die Datenübermittlung kann schriftlich, mündlich, automatisiert oder auf Datenträgern erfolgen. Für den Versand von Daten auf elektronischen Speichermedien oder über eine elektronische Verbindung durch öffentlich zugängliche Netze sind die personenbezogenen Daten auf eine geeignete, dem jeweiligen Stand der Technik entsprechende Weise vor unautorisierten Zugriffen zu schützen.

§ 6
Datenübermittlung bei einem Schulwechsel

(1) Bei einem Schulwechsel übergibt die abgebende Schule der aufnehmenden Schule die Berechtigung zum Zugriff auf die Schülerdaten in der Lehrer- und Schülerdatenbank (LUSD). Insoweit gehen alle Rechte und Pflichten einer datenverarbeitenden Stelle auf die aufnehmende Schule über.

(2) Papiergebundene Unterlagen der Schülerdatei (Schülerakte) werden bei einem Schulwechsel innerhalb von allgemeinbildenden Schulen der aufnehmenden Schule übergeben. Diese hat insbesondere zu überprüfen, ob die ihr übergebenen Daten für die schulische Arbeit erforderlich sind. Die nicht mehr benötigten Unterlagen sind zu vernichten.

§ 7
Datenübermittlung zum Zwecke der Berufsschulpflichtüberwachung

Im Rahmen der Überwachung der Berufsschulpflicht können Schulen den Ausbildungsstellen oder Arbeitgebern unentschuldigte Schulversäumnisse mitteilen.

§ 8
Datenübermittlung zum Zwecke der Gesundheitspflege

(1) Im Rahmen der Schulgesundheitspflege nach Maßgabe der Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege, insbesondere bei der Einschulung und der Entlassung sowie für Untersuchungen zur Schulzahnpflege, übermitteln Schulen dem Gesundheitsamt personenbezogene Daten von Schülerinnen und Schülern sowie der Eltern.

(2) Folgende Daten der Betroffenen werden übermittelt:

1. Vor- und Familienname,
2. Geburtsdatum,
3. Anschrift,
4. Name und (falls von Nr. 3 abweichend) Anschrift der Eltern.

§ 9
Datenübermittlung an das Jugendamt

Die Übermittlung von personenbezogenen Daten und weiteren Sozialdaten an das Jugendamt erfolgt unter den Voraussetzungen des § 62 Abs. 3 des Achten Buches Sozialgesetzbuch.

§ 10
Aufbewahrungsfristen und Löschung von Daten, Vernichtung von Akten

(1) In Schulen sind personenbezogene Daten nur so lange aufzubewahren, wie sie für die Erfüllung des Bildungs- und Erziehungsauftrags, die Erteilung zulässiger Auskünfte oder für das Ausstellen von Bescheinigungen erforderlich sind. Die Aufbewahrungsfristen richten sich nach Anlage 3. Im Übrigen wird die Erforderlichkeit durch die Erfüllung der jeweiligen Aufgabe bestimmt.

(2) Wird eine Schule geschlossen, werden die dauerhaft aufzubewahrenden Unterlagen nach Anlage 3 dem zuständigen Staatsarchiv nach Anlage 3 B Nr. 7 angeboten. Lehnt dieses die Übernahme ab, regelt der Schulträger die Aufbewahrung. Noch befristet aufzubewahrende Dateien werden entweder der Schule übergeben, die die Funktion der geschlossenen Schule übernimmt oder es wird durch den Schulträger im Benehmen mit dem zuständigen Staatlichen Schulamt ein Aufbewahrungsort festgelegt.

(3) Die in privaten Datenverarbeitungseinrichtungen oder Speichermedien der Lehrkräfte gespeicherten personenbezogenen Daten sind zu löschen, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist, spätestens jedoch ein Jahr nach dem Ende des jeweiligen Schuljahres.

(4) Akten, Unterlagen und Daten, deren Aufbewahrungsfristen abgelaufen sind, müssen nach Abstimmung mit dem zuständigen Staatsarchiv unverzüglich vernichtet werden. In automatisierten Verfahren gespeicherte Daten sind zu löschen.

(5) Zur Führung einer Schulchronik (Daten zur Schulgeschichte) dürfen Schulen die folgenden personenbezogenen Daten von Schülerinnen und Schülern zeitlich unbefristet speichern:

1. Vor- und Familienname,
2. Geburtsdatum,
3. Geschlecht,
4. letzte Anschrift während des Schulbesuchs,
5. Daten über die Schulbesuchsdauer.

§ 11
Schulische Datenschutzbeauftragte

(1) Die Schulleitung bestellt die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Schule sowie eine Vertreterin oder einen Vertreter. Die Bestellung soll nach Erwerb oder Nachweis der nach § 5 Abs. 1 des Hessischen Datenschutzgesetzes erforderlichen Sachkenntnis im Einverständnis mit den Betroffenen erfolgen. Sie erfüllen die gesetzlichen Aufgaben als Datenschutzbeauftragte nach § 5 Abs. 2 des Hessischen Datenschutzgesetzes im Rahmen ihres Beschäftigungsverhältnisses.

(2) Schulleiterinnen und Schulleiter sowie ihre Stellvertreterinnen und Stellvertreter können nicht zu Datenschutzbeauftragten bestellt werden.

(3) Für mehrere Schulen können unbeschadet der Vorschrift des § 5 Abs. 3 Satz 1 des Hessischen Datenschutzgesetzes durch die Schulleiterinnen und Schulleiter gemeinsame Datenschutzbeauftragte bestellt werden. Zum Zuständigkeitsbereich solcher Datenschutzbeauftragten darf höchstens eine Schule mit mehr als 10 Lehrkräften gehören.

(4) Zu den Aufgaben der schulischen Datenschutzbeauftragten nach § 5 des Hessischen Datenschutzgesetzes gehört auch die Beratung der Schülerinnen und Schüler, ihrer Eltern und der Lehrkräfte in Datenschutzangelegenheiten. Dazu gehört auch die Beratung in der Anwendung des Hessischen Datenschutzgesetzes. Sie erstreckt sich darüber hinaus auf die Beratung in der Anwendung anderer Vorschriften zur Regelung der Verarbeitung personenbezogener Daten. Im Rahmen dieser Tätigkeit informieren schulische Datenschutzbeauftragte insbesondere neu eintretendes Personal über die in der Schule wesentlichen Datenschutzvorschriften.

(5) Die oder der schulische Datenschutzbeauftragte prüft jährlich, ob erforderliche Löschungen vollzogen worden sind.

(6) Die oder der schulische Datenschutzbeauftragte überwacht nach § 5 Abs. 2 des Hessischen Datenschutzgesetzes neben der Einhaltung datenschutzrechtlicher Vorschriften auch stichprobenartig die Beachtung des § 10 Abs. 2 des Hessischen Datenschutzgesetzes.

§ 12
Organisation des Datenschutzes

In den Schulen ist sicherzustellen, dass

1. Verfahrensbeschreibungen und Geräteverzeichnis regelmäßig aktualisiert werden,
2. regelmäßig Aufklärung aller in der Schule Beschäftigten über notwendige Datensicherheitsmaßnahmen und die Wahrung des Datengeheimnisses durchgeführt werden,
3. keine unbekannten Datenträger benutzt werden,
4. Akten, Ausdrucke und Datenträger mit personenbezogenen Daten datenschutzgerecht entsorgt werden.

ZWEITER TEIL
Statistische Erhebungen an Schulen

§ 13
Anwendungsbereich

Zum Zweck der Bildungsplanung, der Bildungsberichterstattung, der Evaluierung und der amtlichen Statistik können nach § 85 des Hessischen Schulgesetzes an den öffentlichen Schulen und an den Schulen in freier Trägerschaft statistische Erhebungen durch das Hessische Kultusministerium und das Hessische Statistische Landesamt durchgeführt werden.

§ 14
Periodizität und Berichtszeitpunkt der Erhebungen

(1) Folgende Erhebungen werden mindestens einmal jährlich durchgeführt:

1. Prognosedaten für das folgende Schuljahr einschließlich Anmeldungen an weiterführende Schulen
2. Schulabgänger
3. Landesschulstatistik
4. Zentrale Abschlussprüfungen
5. Landesabitur
6. Unterrichtssituation
7. Vorlaufkurse und Schulanmeldungen

(2) Die Erhebungen einschließlich der genauen Erhebungszeitpunkte werden vom Hessischen Kultusministerium festgelegt. Die Erhebungszeitpunkte orientieren sich an den Terminen der jeweils erhobenen Sachverhalte. Die Erhebungszeitpunkte derjenigen Erhebungen, die auch zu Zwecken der amtlichen Statistik durchgeführt werden, werden im Einvernehmen mit dem Hessischen Statistischen Landesamt festgelegt.

(3) Weitere Erhebungen können anlassbezogen durchgeführt werden. Genaue Berichtszeitpunkte, Berichtsfristen und Stichtage werden vom Hessischen Kultusministerium festgelegt.

§ 15
Erhebungsverfahren

(1) Erhebungen werden auf dem Wege eines Datenabzugs aus dem landeseigenen Schulverwaltungsverfahren Lehrer- und Schülerdatenbank (LUSD) von der abgeschotteten Statistikstelle im Hessischen Kultusministerium durchgeführt. Schulen, die an diesem Verfahren teilnehmen, sind verpflichtet, die Daten der Erhebungen über dieses Verfahren zu übermitteln.

(2) Schulen, die nicht an dem Verfahren LUSD teilnehmen, haben die Erhebungsdaten in einem von der die Erhebung durchführenden Stelle zu bestimmenden Format auf elektronischem Wege zu übermitteln.

(3) Daten, die nicht in dem Verfahren LUSD gespeichert sind, können auf anderem Wege erhoben werden.

(4) Die Daten werden im Regelfall als Einzeldatensätze erhoben. Erhebungs- und Hilfsmerkmale sind in der Anlage 2 aufgeführt. Die Datensätze können mit einem eindeutigen verschlüsselten Kennzeichen (Fallnummer) auf Grundlage der Datenbankkennung aus dem Verfahren LUSD versehen werden, das eine Verknüpfung der Datensätze über die einzelnen Erhebungszeitpunkte hinweg erlaubt. Sofern Einzeldatensätze als personenbeziehbar gelten, werden diese ausschließlich durch die abgeschottete Statistikstelle im Hessischen Kultusministerium verarbeitet.

(5) Werden Einzeldaten über das Schulverwaltungsverfahren LUSD erhoben, sind die Hilfsmerkmale zu löschen, bevor eine Übermittlung in das zentrale Verfahren KultusDataWarehouse des Hessischen Kultusministeriums erfolgt.

(6) Werden Einzeldatensätze vom Hessischen Statistischen Landesamt erhoben, sind die Hilfsmerkmale nach Abschluss der Erhebung zu löschen. Eine Übermittlung der Hilfsmerkmale in das Verfahren KultusDataWarehouse des Hessischen Kultusministeriums ist ausgeschlossen.

(7) Für eine länderübergreifende Vorgehensweise bei der Schulstatistik können die Einzeldatensätze zusätzlich mit einem eindeutigen verschlüsselten Kennzeichen (Fallnummer) versehen werden, das auf der Grundlage von Hilfsmerkmalen der Person erzeugt wird. Die Erzeugung der Fallnummer erfolgt außerhalb des Verfahrens KultusDataWarehouse.

(8) Die Plausibilitätsprüfung der erhobenen Daten erfolgt durch die Staatlichen Schulämter und die abgeschottete Statistikstelle im Hessischen Kultusministerium; die Prüfung der Daten, die für statistische Zwecke erhoben werden, wird zusätzlich durch das Hessische Statistische Landesamt durchgeführt. Den prüfenden Stellen werden alle zu diesem Zweck erforderlichen Daten bereitgestellt.

§ 16
Auskunftspflicht

Auskunftspflichtig sind die Schulleiterinnen und Schulleiter. Soweit Daten zu Erhebungsmerkmalen an den betreffenden Einrichtungen nicht im Geschäftsgang entstehen, sind auch die Lehrkräfte und sonstigen an den betreffenden Einrichtungen beschäftigten Personen sowie die Schülerinnen und Schüler, Einzuschulenden, Schulbewerberinnen und Schulbewerber einschließlich ihrer Erziehungsberechtigten gegenüber den Schulleiterinnen und Schulleitern ihrerseits auskunftspflichtig. Die Befragten sind zur wahrheitsgemäßen, vollständigen und fristgerechten

Auskunftserteilung verpflichtet. Die Schulleiterinnen und Schulleiter sind für die Vollständigkeit und Richtigkeit der Daten verantwortlich. Die Auskunftserteilung ist für den Empfänger kostenfrei.

§ 17
Übermittlung der Daten

(1) Das Hessische Kultusministerium übermittelt erhobene Daten nach § 14 für Zwecke der amtlichen Statistik an das Hessische Statistische Landesamt. Die Übermittlung an andere Stellen, insbesondere Staatliche Schulämter, Institut für Qualitätsentwicklung, Schulträger und Kirchen ist zulässig, wenn die Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich sind oder ein berechtigtes Interesse nach § 16 Abs. 3 des Hessischen Landesstatistikgesetzes nachgewiesen werden kann und die übermittelten Daten nicht Zwecken des Verwaltungsvollzuges dienen. Die datenempfangenden Stellen sind für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

(2) Das Hessische Statistische Landesamt kann erhobene Daten für Zwecke nach § 13 auf Anforderung an das Hessische Kultusministerium übermitteln. Ausgenommen davon sind Einzeldatensätze der Lehrkräfte an Schulen in freier Trägerschaft.

(3) Einzeldatensätze von Lehrkräften an Schulen in freier Trägerschaft, die nach § 15 Abs. 1 vom Kultusministerium erhoben werden, dürfen nur vom Hessischen Statistischen Landesamt ausgewertet werden.

DRITTER TEIL
Schlussvorschriften

§ 18
Aufhebung früherer Vorschriften; Inkrafttreten; Außerkrafttreten

(1) Die Verordnung über die Verarbeitung personenbezogener Daten in Schulen vom 30. November 1993 (ABl. 1994 S. 114, ber. S. 206) wird aufgehoben.

(2) Diese Verordnung tritt am Tage nach der Verkündung in Kraft. Sie tritt mit Ablauf des 31. Dezember 2014 außer Kraft.

Anlage 1 zur Verarbeitung personenbezogener Daten in Schulen

A Personenbezogene Schülerdaten

1. Grunddaten der Schülerin oder des Schülers

1.1 Allgemeines Schüleraktenzeichen,
1.2 Name; gegebenenfalls auch der Geburtsname,
1.3 Vorname,
1.4 Anschrift,
1.5 Telefonnummer, Telefaxnummer und E-Mail-Adresse, sofern der Erhebung nicht durch die Eltern oder die volljährige Schülerin oder den volljährigen Schüler widersprochen wird,
1.6 Geschlecht,
1.7 Geburtsdatum und -ort, Land,
1.8 Konfession, sofern Religionsunterricht dieser Religionsgemeinschaft in Hessen erteilt wird und keine Abmeldung gemäß § 8 Abs. 3 des Hessischen Schulgesetzes vorliegt,
1.9 Staatsangehörigkeit (einschließlich Spätaussiedlereigenschaft, Familien-/Muttersprache, Jahr des Zuzugs in die Bundesrepublik),
1.10 Ausbildungsbetrieb,
1.11 Namen, Namenszusatz der Eltern,
1.12 Vornamen der Eltern,
1.13 Anschrift der Eltern,
1.14 Telefonnummer, Telefaxnummer und E-Mail-Adresse der Eltern, sofern der Erhebung durch diese nicht widersprochen wird,
1.15 auf Wunsch der Eltern die Kommunikationsmöglichkeit, über die im Notfall eine Entscheidung über notwendige Maßnahmen herbeigeführt werden kann,
1.16 Vermerk über schulische Funktion der Eltern,
1.17 Erziehungsberechtigung,
1.18 Erziehungsvereinbarungen.

2. Organisations- und Schullaufbahndaten

2.1 Datum der Einschulung,
2.2 Eintrittsdatum,
2.3 Qualifikationen, Bildungsnachweise,
2.4 bisher besuchte Schulen (Zeiträume, Schulname, Schulnummer, Anschriften mit Schulartangabe, anderes Bundesland),
2.5 Klassenbezeichnung, Jahrgangsstufe, Halbjahr und gegebenenfalls erfolgter Klassenwechsel/wiederholte Klassen/Begrenzung der Verweildauer,
2.6 Klassenlehrer, Tutor,
2.7 Entlassungsdatum (Aushändigungsvermerk des Zeugnisses) und Art des erstellten Zeugnisses (erreichter Abschluss/ Abschlussprüfung),
2.8 Anmeldung an weiterführende Schulen, Datum der Anmeldung, Schule, Erst- und weitere Wahlen,

2.9 Überweisungsdatum, Name, Anschrift der aufnehmenden Schule,
2.10 Befreiung vom Unterricht, insbesondere vom Sportunterricht (Umfang/Zeitraum); sofern an der Schule Religionsunterricht erteilt wird, Datum der An- oder Abmeldung vom Religionsunterricht, Wiederanmeldung sowie Teilnahme am Religionsunterricht eines anderen Bekenntnisses,
2.11 Schulversäumnisse,
2.12 individuelle Förderpläne,
2.13 Beurlaubung vom Schulbesuch für mehr als zwei Monate innerhalb einer Jahrgangsstufe,
2.14 Abmeldung vom Schulbesuch,
2.15 Neuanmeldung zum Schulbesuch nach gewähltem Schwerpunkt bei Ausbildungsgängen mit alternativen Schwerpunktmöglichkeiten,
2.16 Fremdsprachenbelegung (einschließlich erreichter Abschlüsse),
2.17 Kurswahl in den Wahlpflichtbereichen ab Jahrgang 7,
2.18 Kurszuweisung in Fächern mit Fachleistungsdifferenzierung,
2.19 besondere gesundheitliche Beeinträchtigung und körperliche Behinderung; Teilnahme an erforderlichen Untersuchungen,
2.20 Teilnahme an zusätzlichen freiwilligen Unterrichtsveranstaltungen und Arbeitsgemeinschaften (Beginn und Ende), insbesondere Daten zur Teilnahme an Fördermaßnahmen (wie LRS-Förderung, Deutsch für ausländische Schülerinnen und Schüler, Sprachheilunterricht), Teilnahme am herkunftssprachlichen Ergänzungsunterricht,
2.21 Praktika (Zeitraum, Ausbildungsstätte und Anschrift),
2.22 Schülerbeförderung und Art der Beförderung (Schulweg in km, Verkehrsverbindung; Beförderung mit dem Schulbus, mit öffentlichen Verkehrsmitteln; Bewilligungszeitraum, ausgestellte Schülerfahrscheine),
2.23 Mandat in Mitwirkungsorganen,
2.24 sonstige schulbezogene Funktionen der Schülerin oder des Schülers,
2.25 Ehrenamtsdaten, sofern die oder der Betroffene bzw. die Eltern dies wünschen,
2.26 Auslandsaufenthalt,
2.27 BAföG-Schulbescheinigung (Datum und Kennzeichen),
2.28 Eignungsfeststellung für den Besuch einer weiterführenden Schule,
2.29 Schüler-Zusatzversicherungen,
2.30 Erziehungs- und Ordnungsmaßnahmen, soweit nach § 82 Abs. 10 des Hessischen Schulgesetzes zulässig.

3. Leistungsdaten

3.1 Zeugnisnoten, Versetzungsentscheidungen, Zertifikate und Ergebnisse von Prüfungen,
3.2 Angaben über Benachrichtigungen bei gefährdeter Versetzung einschließlich des Hinweises auf etwaige besondere Folgen einer Nichtversetzung,
3.3 Zeitpunkt und Ergebnis von Versetzungs- und Klassenkonferenzen; Versetzung, Wiederholung, Überspringen einer Jahrgangsstufe, gegebenenfalls Laufbahnempfehlung für den Übergang in eine andere Schulart, Zulassung zur Prüfung/Nachprüfung/Wiederholungsprüfung,

erreichter oder zuerkannter Abschluss; Ergebnis anderer Zeugnis- und Laufbahnkonferenzen.

4. Schulartspezifische Zusatzdaten

4.1 Grundschule

4.1.1 Zurückstellung vom Schulbesuch (Dauer und Grund),
4.1.2 Besuch einer Vorklasse einschließlich Anrechnung der Zeit der Zurückstellung auf die Dauer der Schulpflicht,
4.1.3 vorzeitige Aufnahme einschließlich Untersuchungsergebnis,
4.1.4 Vorlaufkurse,
4.1.5 Ergebnis der Einschulungsuntersuchung,
4.1.6 Anträge und Gutachten für den sonderpädagogischen Förderbedarf in der Integrationsklasse, sonderpädagogische Förderung in der Integrationsklasse,
4.1.7 Schullaufbahnempfehlung.

4.2 Schulen der Mittelstufe

4.2.1 Fächer des Wahlpflichtunterrichts,
4.2.2 Kurseinstufungen,
4.2.3 Einzelergebnisse der Abschlussprüfung in der Mittelstufe.

4.3 Gymnasiale Oberstufe

4.3.1 Kurswahl Oberstufe, Abiturfächer und Leistungsergebnisse,
4.3.2 Leistungsbewertungen,
4.3.3 Fremdsprachen (Art und Zeitraum in Mittel- und Oberstufe),
4.3.4 Wahlpflichtunterricht,
4.3.5 Zulassung zum Abitur (erforderliche Ergebnisse und Datum),
4.3.6 Wahl der Prüfungsfächer zum Abitur,
4.3.7 Fächer mit schriftlichen Arbeiten,
4.3.8 Wahl der Prüferinnen und Prüfer zum Abitur,
4.3.9 Einzelergebnisse im Abitur,
4.3.10 besondere Berechtigungen (zum Beispiel Latinum, Graecum, Hebraicum),
4.3.11 Feststellungsprüfungen in Fremdsprachen.

4.4 Berufsschule

4.4.1 Ausbildungsberuf, gegebenenfalls Schwerpunkt,
4.4.2 Ausbildungs-/Arbeitszeitraum (Eintrittsdatum bei Betrieb/Folgebetrieb, Bildungsträger, Ausbildungsmonate, voraussichtliches Ende der Ausbildung, Verkürzung oder Verlängerung der Ausbildung nach § 29 des Berufsbildungsgesetzes, Ausbildungsende),
4.4.3 Art des Ausbildungsverhältnisses/Berufstätigkeit (Berufsfeld oder Fachrichtung),

4.4.4 Bezeichnung der Ausbildungsstätte/Arbeitsstätte mit Anschrift und Telefonverbindung, Amtsbezirk, „zuständige Stelle“ nach dem Berufsbildungsgesetz,
4.4.5 frühere Berufsausbildung,
4.4.6 angestrebter schulischer Abschluss,
4.4.7 Anwesenheitsliste,
4.4.8 Berufsschultage,
4.4.9 Voll- oder Teilzeitschule, Blockunterricht,
4.4.10 Einzelergebnisse der Abschlussprüfung in der Berufsschule.

4.5 Förderschule

4.5.1 Aufnahmeverfahren (Datum und Entscheidung),
4.5.2 Ergebnisse der schulärztlichen, schulpsychologischen oder sonderpädagogischen Gutachten,
4.5.3 Anträge zur Festlegung von sonderpädagogischem Förderbedarf,
4.5.4 Gutachten über den sonderpädagogischen Förderbedarf (nach erfolgter Diagnostizierung mit Beschulungsvorschlag /Schullaufbahnempfehlung),
4.5.5 sonderpädagogische Gutachten nach der Beobachtungszeit: Anamnese der Schülerin oder des Schülers in ihrer oder seiner Familie (Alter der Eltern, Anzahl der Geschwister), Sprache (Sprachentwicklung, Sprachzustand, Sprachverhalten), Motorik (motorische Entwicklung, Bewegungsverhalten), Lernverhalten (Aufmerksamkeit, Konzentration, Merkfähigkeit, Gedächtnis, Aufgabenverständnis, Problemlösungsverhalten, Mitarbeitsbereitschaft, Arbeitstempo, Ausdauer), affektiv-emotionales und soziales Verhalten (Kontaktfähigkeit, Bindungsfähigkeit, Spielverhalten, Verhalten in sozialen Anforderungssituationen usw.), Handlungsfähigkeit in Situationen der täglichen Erfahrung, zusammenfassende Beurteilung, Förderempfehlungen, individuelle Förderplanung,
4.5.6 jährlicher Entwicklungs- und Leistungsbericht, prozessbegleitende Förderdiagnostik.

4.6 Schulen mit Heim

4.6.1 Aufnahmeverfahren (Datum und Entscheidung),
4.6.2 Krankenkasse,
4.6.3 Vorerkrankungen,
4.6.4 Gesundheitszeugnis.

5. Inhalt der Klassenbücher

Das Klassenbuch oder das Kursheft kann die folgenden Angaben enthalten:

5.1 Bezeichnung der Klasse oder des Kurses,
5.2 Namen und ggf. klasseninterne Funktionen der unterrichtenden Lehrkräfte unter Nennung der Fächer mit planmäßiger Wochenstundenanzahl,
5.3 Sprechstunden der in der Klasse unterrichtenden Lehrkräfte,

5.4 Namen der Schülerinnen und Schüler einschließlich schulischer Funktionen,
5.5 Teilnahme an nicht im Klassenverband erteiltem Unterricht,
5.6 Angaben über den Klassenelternbeirat,
5.7 Nachweise zum Unterricht, Vermerke über Schulversäumnisse (entschuldigt/unentschuldigt), Verspätungen,
5.8 besondere Vorkommnisse im Unterricht,
5.9 Stundenplan,
5.10 Stunden- oder Wochenbericht unter Angabe der Unterrichtsinhalte und/oder Unterrichtsziele,
5.11 Schulische Veranstaltungen außerhalb des Unterrichts, insbesondere Wandertage, Landheimaufenthalte, Studienreisen und Ähnliches.

6. Datensatz bei der Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

6.1 Name einschließlich Geburtsname,
6.2 Vorname,
6.3 Geschlecht,
6.4 Geburtsdatum,
6.5 Klasse/Jahrgangsstufe, Kurs,
6.6 Schüleraktenzeichen und Gesamtschülerverzeichnis,
6.7 LUSD-ID der Schülerin oder des Schülers,
6.8 Unterrichtsfächer,
6.9 Bildungsgang, Ausbildungsrichtung/Ausbildungsberuf, gegebenenfalls Schwerpunkt,
6.10 Fächer, in denen die Lehrkraft Schülerinnen und Schüler unterrichtet,
6.11 selbst erteilte Zeugnisnoten und Ergebnisse und Teilergebnisse schriftlicher, mündlicher und praktischer Leistungsüberprüfungen sowie Verhaltensbewertungen in dem von der Lehrkraft erteilten Unterricht sowie Art und Datum der Leistungserhebung beziehungsweise der Bewertung,
6.12 Zeiten des Fernbleibens vom Unterricht in den Fächern, in denen die Lehrkraft die Schülerinnen und Schüler unterrichtet,
6.13 Mitglieder der Schulleitung, gegebenenfalls weitere mit Leitungsaufgaben betraute Lehrkräfte und Klassenlehrer dürfen soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, darüber hinaus die folgenden Schülerdaten verarbeiten:
6.13.1 Halbjahresnoten in allen Fächern der betreffenden Schülerinnen und Schüler,
6.13.2 alle zeugnisrelevanten Leistungsangaben,
6.13.3 zeugnisübliche Bemerkungen,
6.13.4 Telefonnummer, Telefaxnummer und E-Mail-Adresse der Schülerinnen und Schüler sowie deren Eltern, sofern der Erhebung nicht widersprochen wird,
6.14 Förderschullehrkräfte und Berufsschullehrkräfte mit sonderpädagogischer Zusatzausbildung dürfen zur Erstellung von sonderpädagogischen Gutachten außerdem folgende personenbezogene Daten verarbeiten:
6.14.1 zur Anamnese der Schülerin oder des Schülers in ihrer oder seiner Familie,
6.14.2 zu den Entwicklungsbedingungen der Lernumwelt,
6.14.3 zu Faktoren und Merkmalen hinsichtlich der Vorgeschichte,

6.14.4 zu Lernvoraussetzungen und den individuellen Fähigkeiten in ihrem Zusammenhang mit der aktuellen Lernsituation,
6.14.5 zum Lernverhalten,
6.14.6 zur sprachlichen Entwicklung,
6.14.7 zur körperlichen und motorischen Entwicklung,
6.14.8 zum emotionalen und sozialen Verhalten,
6.14.9 zur kognitiven Entwicklung,
6.14.10 zur Handlungsfähigkeit in Situationen der täglichen Erfahrung,
6.14.11 zu zusammenfassenden Beurteilungen,
6.14.12 zu Förderempfehlungen und zu Hinweisen für den zu entwickelnden Förderplan.

B Personenbezogene Daten der Lehrkräfte

1 Name, gegebenenfalls Namenszusatz, Geburtsname, Vorname(n),
2 Personalnummer,
3 Geschlecht,
4 Anschrift,
5 Telefon, gegebenenfalls Telefax und E-Mail-Adresse,
6 Nationalität,
7 Amts-/ Dienstbezeichnung,
8 Rechtsstellung,
9 Lehramt,
10 Funktion innerhalb der Schule,
11 Beauftragungen,
12 Stammdienststelle,
13 Lehrbefähigung (jeweils Fach und Art),
14 Unterrichtserlaubnis (Art und Ablauftermin),
15 Unterrichtseinsatz (Wochenstunden, Fächer, Klassen/Kurse),
16 Pflichtstundensoll/Regelpflichtstunden,
17 Mehrarbeit,
18 Unterricht an anderen Schulen (Schule, Schulform, Wochenstunden, Fächer, Klassen/Kurse),
19 Anrechnung dienstlicher Tätigkeiten (Wochenstunden, Grund),
20 Pflichtstundenermäßigung (Wochenstunden, Grund),
21 Schwerbehinderung, Nachteilsausgleich,
22 abweichende Arbeitszeitregelung (Altersteilzeit, Sabbatjahr),
23 Freistellungen,
24 Sprechstunde (Tag, Zeit, Raum),
25 Schuleintrittsdatum,
26 Fortbildungen,
27 bei Lehrkräften im Vorbereitungsdienst: Examensdaten.

Anlage 2 zu statistischen Erhebungen an Schulen

A Schüler- und Unterrichtsdaten

1. Daten der Schülerin oder des Schülers

1.1 Name (Hilfsmerkmal),
1.2 Vorname (Hilfsmerkmal),
1.3 Wohnort (Gemeindekennziffer),
1.4 LUSD-ID (Hilfsmerkmal),
1.5 Geschlecht,
1.6 Jahr der Ersteinschulung,
1.7 Eintrittsdatum in die Schule,
1.8 Zurückstellungen,
1.9 Geburtstag (Hilfsmerkmal) ,-monat und -jahr, Land der Geburt,
1.10 Staatsangehörigkeiten,
1.11 Zuzug in die Bundesrepublik,
1.12 Verkehrssprache in der Familie,
1.13 Konfession,
1.14 Abmeldung vom Religionsunterricht,
1.15 besuchter Bildungsgang,
1.16 besuchte Jahrgangsstufe,
1.17 Fachrichtung, Schwerpunkt,
1.18 Ausbildungsberuf,
1.19 Ort des Ausbildungsbetriebes,
1.20 schulische Vorbildung,
1.21 vorherige Berufsausbildungen,
1.22 besuchte Schule,
1.23 Beurlaubung,
1.24 besuchte Klasse,
1.25 besuchte Unterrichts- und sonstige schulische Veranstaltungen,
1.26 im Vorjahr besuchte Schule, Schulform und Jahrgangsstufe,
1.27 zuletzt besuchte Schule, Schulform und Jahrgangsstufe,
1.28 Art und Zeitpunkt erreichter schulischer Abschlüsse,
1.29 Versetzungen und Nichtversetzungen,
1.30 Anmeldungen an weiterführende Schulen,
1.31 Empfehlungen zur Schullaufbahn,
1.32 sonderpädagogische Förderung,
1.33 Fremdsprachenfolgen,
1.34 Teilnahme an Prüfungen und Leistungsstandsmessungen,
1.35 Prüfungsfächer und -ergebnisse,
1.36 Prüfungsaufgaben und -ergebnisse,
1.37 Zeugnisfächer und -noten,
1.38 vorschulische Förderung und Ergebnisse.

2. Klassen

2.1 Bezeichnung der Klasse,
2.2 Bildungsgang,
2.3 Jahrgangsstufe,
2.4 Art der Klasse,
2.5 erteilte Unterrichts- und sonstige schulische Veranstaltungen.

3. Unterrichtsveranstaltungen

3.1 Bezeichnung (Hilfsmerkmal),
3.2 Bildungsgang,
3.3 Jahrgangsstufe,
3.4 Art der Veranstaltung,
3.5 Umfang und Dauer,
3.6 Fachinhalt,
3.7 Thema,
3.8 Differenzierungen,
3.9 besondere Eigenschaften,
3.10 teilnehmende Schülerinnen und Schüler,
3.11 erteilende Lehrkräfte und sonstiges Personal (nur an öffentlichen Schulen).

B Daten der Lehrkräfte

1 Name (Hilfsmerkmal),
2 Vorname (Hilfsmerkmal),
3 Personalnummer (Hilfsmerkmal),
4 Geschlecht,
5 Geburtstag (Hilfsmerkmal), -monat und -jahr,
6 Staatsangehörigkeiten,
7 Qualifikationen,
8 Funktionen (Planstellenmerkmale),
9 Beschäftigungs-/Vertragsverhältnisse,
10 Regelpflichtstunden,
11 Vertragsumfang/vertragliche Arbeitszeit,
12 Mehr- und Minderstunden aus Arbeitszeitregelungen,
13 nicht unterrichtswirksame Stunden,
14 Abordnungen,
15 Versetzungen,
16 Vertretungen,
17 Zugangsart,
18 Abgangsart,
19 Klassenlehrer,
20 erteilte Unterrichtsveranstaltungen (nur an öffentlichen Schulen),
21 Stammdienststelle.

C Daten der Schulen

1 Bezeichnung,
2 Ort,
3 Adress- und Kommunikationsdaten,
4 Schulträger,
5 Fachaufsicht,
6 Rechtsstellung,
7 Organisationsform,
8 angebotene Bildungsgänge,
9 besondere Einrichtungen.

Anlage 3 Aufbewahrung, Aussonderung und Archivierung

A Aufbewahrungsfristen

1. Dauernd aufzubewahren sind
1.1 Schulprogramme - dazu zählen in Schulen bereits als Schulprogramm beschriebene regelmäßige Entwicklungsberichte und verpflichtende Schulprogramme, wenn sie gesetzlich eingeführt werden -,
1.2 Jahresberichte und Festschriften,
1.3 Schulchroniken.

2. Fünfzig Jahre aufzubewahren sind
2.1 die Schülerkarte,
2.2 Zweitschriften von Abgangs- und Abschlusszeugnissen,
2.3 die Hauptakte der Schulakten.

3. Dreißig Jahre aufzubewahren sind Protokolle der Gesamt- und Schulkonferenz.

4. Zehn Jahre aufzubewahren sind
4.1 Prüfungsakten einschließlich der Prüfungsarbeiten und Gutachten; im Rahmen von Prüfungen angefertigte besondere Hausarbeiten, insbesondere künstlerische Arbeiten, sind auf schriftlichen Antrag, der spätestens ein Jahr nach Abschluss der Prüfung gestellt werden muss, an den Prüfling zurückzugeben,
4.2 die nicht unter Nr. 3 aufgeführten Konferenzprotokolle,
4.3 Bestandsverzeichnisse bei der Durchführung der Lernmittelfreiheit,
4.4 Schulstatistiken.

5. Fünf Jahre aufzubewahren sind
5.1 Lehrberichte,
5.2 Klassen- und Kursbücher,
5.3 die Schülerakte, ausgenommen die unter Nr. 2.1 bis 2.3 aufgeführten Unterlagen,
5.4 Zeugnislisten,
5.5 Schülerverzeichnisse,
5.6 die Rechnungsunterlagen bei der Durchführung der Lernmittelfreiheit.

6. Zwei Jahre aufzubewahren sind
6.1 die Nebenakten der Schulakte,
6.2 Versäumnislisten,
6.3 Notenbücher oder entsprechende von Lehrkräften außerhalb der Schule geführte Ergebnislisten,
6.4 Schulbesuchsbescheinigungen im Rahmen der Schülerförderung (BAföG).

7. Die Fristen gelten auch für automatisiert gespeicherte Dateien.

8. Die Aufbewahrungsfrist beginnt mit dem Schluss des Jahres, in dem die Listen, schriftlichen Nachweise, Statistiken, Verzeichnisse, Lehrberichte und Klassenbücher abgeschlossen wurden. Sie beginnt bei Unterlagen, die einzelne Schülerinnen und Schüler betreffen, mit dem Schluss des Jahres, in dem die Schülerin oder der Schüler aus der Schule ausgeschieden ist, falls Rechtsmittel eingelegt worden sind, mit dem Schluss des Jahres, in dem das Rechtsmittelverfahren abgeschlossen worden ist.

9. Die Aufbewahrung erfolgt in dafür geeigneten Räumen der Schule, ausgenommen die nach Nr. 6.3 außerhalb der Schule geführten und aufbewahrten Nachweise. Die Unterlagen sind vor dem Zugriff unbefugter Dritter ausreichend zu sichern.

10. Unabhängig von den Aufbewahrungsfristen sind besondere Vorschriften zur Löschung von Unterlagen wie die des § 82 Abs. 10 des Hessischen Schulgesetzes hinsichtlich der Eintragungen und Vorgänge über Ordnungsmaßnahmen zu beachten.

B Aussonderung und Archivierung

1. Geschlossene und abgelegte Akten und schriftliche Unterlagen sind ab Beginn ihrer Aufbewahrung mit einem deutlichen Hinweis über das Ende der Aufbewahrungsfrist zu versehen. Möglichst jährlich, längstens in Abständen von zwei Jahren ist zu überprüfen, für welches Schriftgut die Aufbewahrungsfrist abgelaufen ist.

2. Nach Ablauf der Frist ist das Schriftgut auszusondern und dem zuständigen Staatsarchiv zur Übernahme anzubieten (§§ 10 ff. des Hessischen Archivgesetzes). Dieses entscheidet unverzüglich über die Archivwürdigkeit und übernimmt das Schriftgut, das für archivwürdig angesehen wird. Lehnt das Archiv die Übernahme ab oder entscheidet es nicht innerhalb eines Jahres über die Archivwürdigkeit, ist das Schriftgut zu vernichten, sofern kein Grund zu der Annahme besteht, dass durch die Vernichtung schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Das Gleiche gilt für Dateien in elektronischer Form vor der Löschung.

3. Regelmäßig werden als archivwürdig übernommen Schulprogramme, Jahresberichte, Festschriften und Schulchroniken bei Auflösung der Schule.

4. Den Archiven werden regelmäßig angeboten
4.1 Schülerkarte,
4.2 Zweitschriften von Abgangs- und Abschlusszeugnissen,
4.3 Prüfungsakten mit den dazugehörigen Prüfungsarbeiten und Gutachten,
4.4 Hauptakten der Schulakte,
4.5 Konferenzprotokolle,
4.6 Bestandsverzeichnisse bei der Durchführung der Lernmittelfreiheit,
4.7 Schulstatistiken,

4.8 alle Akten und sonstigen Unterlagen, die seit 1950 nicht mehr weitergeführt worden sind.

5. Die Staatsarchive können mit einzelnen Schulen Sondervereinbarungen über die Archivierung treffen.

6. Das nicht unter Nr. 3, 4 und 5 erfasste Schriftgut, insbesondere die Stundenpläne, Lehrberichte, Zeugnislisten, Nachweise über schriftliche Arbeiten, Versäumnislisten, Klassen- oder Kursbücher und Schulbesuchsbescheinigungen, sind nach Ablauf der Aufbewahrungsfrist auszusondern und zu vernichten.

7. Die zuständigen Staatsarchive sind
7.1 das Hessische Hauptstaatsarchiv Wiesbaden für die Städte Frankfurt am Main und Wiesbaden, den Hochtaunuskreis, den Lahn-Dill-Kreis, den Landkreis Limburg-Weilburg, den Main-Kinzig-Kreis, den Main-Taunus-Kreis und den Rheingau-Taunus-Kreis,
7.2 das Hessische Staatsarchiv Darmstadt für die Städte Darmstadt und Offenbach am Main, die Landkreise Bergstraße, Darmstadt-Dieburg, Gießen, Groß-Gerau und Offenbach, den Odenwaldkreis, den Vogelsbergkreis und den Wetteraukreis,
7.3 das Hessische Staatsarchiv Marburg für die Stadt Kassel und die Landkreise Fulda, Hersfeld-Rotenburg, Kassel, Marburg-Biedenkopf und Waldeck-Frankenberg, den Schwalm-Eder-Kreis und den Werra-Meißner-Kreis.

8. Das unter Nr. 3 und Nr. 4 aufgeführte Schriftgut wird grundsätzlich den zuständigen Staatsarchiven angeboten; diese können mit kommunalen oder anderen öffentlichen Archiven vereinbaren, die Archivierung dort vorzunehmen.

9. Die Vernichtung des ausgesonderten und nicht vom Staatsarchiv übernommenen Schriftguts obliegt der Schule. Die Abwicklung kann durch den Schulträger erfolgen. Über die Vernichtung ist eine Niederschrift aufzunehmen; sie ist dauernd aufzuheben. Nach Abschnitt A Nr. 6.3 außerhalb der Schule geführte Nachweise können von der sie verwahrenden Lehrkraft vernichtet werden; dies ist der Schulleiterin oder dem Schulleiter schriftlich anzuzeigen.

10. Soweit in dieser Anlage keine Regelungen getroffen sind, gilt der gemeinsame Erlass - Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen vom 4. Dezember 1996 (StAnz. S. 4275) - in der jeweiligen Fassung.

1.3 Erlasse des Hessischen Kultusministeriums

1.3.1 Erlass über die Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft

vom 21. August 2009 (ABl. 2009 S. 726)

Die Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 ermöglicht gemäß § 3 die Verarbeitung personenbezogener Daten auch automatisiert am häuslichen Arbeitsplatz, sofern diese Daten für die dienstliche Tätigkeit notwendig sind und die notwendigen Sicherungsmaßnahmen im Sinne des § 10 des Hessischen Datenschutzgesetzes eingehalten werden. Die Tatsache der häuslichen Verarbeitung ist der Schulleitung anzuzeigen. Ein beispielhaftes Formblatt für diese Anzeige ist diesem Erlass als Anhang beigefügt.
Voraussetzung für die Nutzung des häuslichen Arbeitsplatzes ist die Gewährleistung eines IT-Sicherheitsstandards, der dem Schutzbedarf der Daten nach Anlage 1. A 6 der o.a. Verordnung Rechnung trägt.
Der häusliche Arbeitsplatz genügt dann den Anforderungen an IT-Sicherheit und Datenschutz, wenn folgende Bedingungen erfüllt sind:

- Der genutzte Rechner verfügt über einen aktuellen Schutz vor Schadprogrammen.
- Der häusliche Arbeitsplatz ist so einzurichten, dass während der Nutzung des häuslichen Rechners die personenbezogenen Daten von Unbefugten nicht eingesehen werden können.
- Wird die Bearbeitung von personenbezogenen Daten unterbrochen, ist der Zugang zum Rechner und zu den Daten durch den Anwender bzw. die Anwenderin zu sperren. Ein passwortgeschützter Bildschirmschoner ist zu aktivieren.
- Der Zugriff zu den gespeicherten personenbezogenen Daten ist kontrollierbar gestaltet (gesicherte Dateiablage mit wirksamem Passwortschutz, verschlüsselte Speicherung). Die Dateiablage erfolgt getrennt von den sonstigen Daten auf einem externen Datenträger, z.B. einer externen Festplatte bzw. einem USB-Stick, der ausschließlich für diesen Zweck genutzt wird und der gesondert und verschlossen aufbewahrt werden kann. Damit können im Bedarfsfall (z.B. plötzliche Dienstunfähigkeit) die Daten problemlos an die Schule zurückgegeben werden.
- Werden personenbezogene Daten auf Datenträgern außerhalb der Wohnung mitgeführt, z.B. beim Transport zur Schule, so sind sie in jedem Fall zu verschlüsseln.
- Arbeitsergebnisse – sofern diese personenbezogene Daten enthalten – sind zeitnah auf die Systeme der Schulverwaltung bzw. in die Schülerakten oder die Schulakten zu übertragen. Danach sind die Daten zu löschen oder die Texte zu anonymisieren. Die Dateiablage ist daher unter diesem Gesichtspunkt regelmäßig zu überprüfen.
- Ist der Rechner in ein Netzwerk eingebunden, ist darauf zu achten, dass die passwortgeschützten und virtuellen Laufwerke bzw. Ordner nicht im Betriebssystem freigegeben sind und damit für andere Anwender sichtbar werden. Bei besonders

gefährdeten Schnittstellen, wie WLAN sind sichere Verschlüsselungsmechanismen zu aktivieren.

Für die Erstellung von Sonderpädagogischen Gutachten am häuslichen Arbeitsplatz macht der Hessische Datenschutzbeauftragte eine Reihe von Vorgaben, die auf seiner Homepage in der Rubrik „Fachthemen/Datenschutz in Schulen“ (www/datenschutz.hessen.de/fachthemen.htm) unter dem Titel „Verarbeitung von Schüler- und Lehrerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte“ eingesehen werden können. Lehrkräfte, die diese Forderungen nicht erfüllen können, müssen die Gutachten entweder handschriftlich, auf einer klassischen Schreibmaschine oder auf einem Verwaltungsrechner in der Schule erstellen. In letzterem Fall sind sie verschlüsselt zu speichern.

Anlage 1: Formblatt zur Anmeldung des häuslichen Arbeitsplatzes

Anlage 2: Handreichung zur Umsetzung der Vorgaben des Erlasses zur Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft

Anlage 1

Formblatt zur Anmeldung des häuslichen Arbeitsplatzes

An die Schulleitung des / der:

_____

Ich beabsichtige mit meinem privaten PC in meinem häuslichen Bereich personenbezogene Daten von Schülerinnen und Schülern nach Anlage I. A 6 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 für dienstliche Zwecke zu verarbeiten. Die Datenverarbeitung dient unmittelbar der Aufgabenerfüllung in meinem pädagogischen Verantwortungsbereich.

Vom Inhalt der o.a. Verordnung habe ich Kenntnis genommen.

Ich sichere zu, dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Kontrollaufgaben in meinem häuslichen Bereich zu ermöglichen. Ich verpflichte mich, dem/der Beauftragten des HDSB nach vorheriger Terminvereinbarung Zugang zu der häuslichen Arbeitsstätte zu gewähren, um die Einhaltung der gebotenen Maßnahmen zur Gewährleistung der IT-Sicherheit und des Datenschutzes zu überprüfen. Diese Zusicherung gilt auch für alle erwachsenen Mitbewohner meines Haushaltes.

Sicherheitsmaßnahmen

- Der Rechner verfügt über einen aktuellen Schutz vor Schadprogrammen
- Der Rechner und der in diesem Zusammenhang genutzte, gesonderte Datenträger sind zugangsgeschützt (Passwort)
- Personenbezogene Daten werden auf diesem Datenträger verschlüsselt gespeichert.

_____

(Unterschrift / Datum)

Anlage 2

Handreichung zur Umsetzung der Vorgaben des Erlasses zur Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft

Die hier folgenden Hinweise sollen den Lehrerinnen und Lehrern helfen, die Vorgaben des vorstehenden Erlasses zu erfüllen und einen ausreichenden Sicherheitsstandard am häuslichen Arbeitsplatz zu gewährleisten.

Maßstab für die Sicherheitsstandards im öffentlichen Bereich sind die Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik (nachfolgend BSI genannt) Link http://www.bsi.de

Die folgenden Hinweise und Empfehlungen greifen daher die Angebote des BSI auf und sollen die Lehrkräfte dazu befähigen, die angebotene Schutzsoftware auf dem häuslichen Rechner zu installieren und zu nutzen.

Im Rahmen der Internetangebote des BSI kann auch ein Newsletter angefordert werden, der schnell und kompetent über die verschiedenen Varianten von Schadsoftware und die aktuellen Sicherheitslücken in Computeranwendungen informiert. Bei Bedarf werden auch Warnmeldungen und Sicherheitshinweise per E-Mail verschickt. Das Abonnement dieses Dienstes ist kostenlos.

Unter dem Menü <BSI für Bürger> werden wichtige Themen zur IT-Sicherheit sehr anschaulich aufbereitet.
Link http://www.bsi-fuer-buerger.de/

Unter dem Menü <Download> werden u.a. Tools zum Thema IT-Sicherheit angeboten, die folgende Bedingungen erfüllen:

- Die Programme (Freeware) dürfen kostenlos (für die private Nutzung) genutzt werden.

- Sie sind grundsätzlich in deutscher Sprache.
- Die Programme erfüllen funktionale und ergonomische Kriterien, das heißt sie sind gebrauchsfähig und einfach in der Handhabung.
  Quelle: BSI für Bürger, http://www.bsi-fuer-buerger.de/

Für die Nutzung des privaten PCs im Rahmen des häuslichen Arbeitsplatzes sind die Themen Internet, Browser, Datensicherung und Schutz vor Viren von besonderer Bedeutung. Ein persönliches Benutzerkonto verhindert, dass Unbefugte den Computer starten können.

Besonders empfehlenswert sind Programme zu den Themen:

- **Virenschutz:** Computerviren sind Schadprogramme, die sich vergleichbar zu Grippeviren in einem menschlichen Organismus in einem Computer ausbreiten und große Schäden anrichten können. Eine Infektion mit einem Computervirus kann mit einem Virenschutzprogramm verhindert werden. Zusätzlich schützt eine Firewall vor einer möglichen Ansteckung mit einem Computervirus.
- **Firewall:** Eine Firewall verhindert bzw. erschwert einen heimlichen Zugang auf den eigenen PC, sobald dieser mit dem Internet verbunden ist. Trotz aller Sicherungen ist aber zu beachten, dass auch eine Firewall keine hundertprozentige Sicherheit vor Angreifern im Internet bietet. Übertragen auf ein praktisches Beispiel kann man eine Firewall auch mit dem Verschließen einer Haustüre oder anderer Hauszugänge vergleichen. Eine offene Türe ist fast schon eine Einladung zu einem Einbruch.
- **Anti-Spy-Tools:** Bestimmte Schadprogramme können sich in dem privaten PC einnisten und das Nutzerverhalten ausspionieren. Diese Spionage kann z.B. darin bestehen, dass persönliche Daten, wie Kontodaten etc. ausgespäht werden. Andere Schadprogramme können z.B. alle Tastendrücke speichern und an kriminelle Personen übermitteln (key-logger). Anti-Spy-Tools können diese Schadprogramme aufspüren und von dem PC entfernen.
- **Verschlüsselungs-Tools:** Mit diesen Programmen können privat genutzte Daten verschlüsselt werden. Hier besteht die Möglichkeit, einzelne Dateien, Verzeichnisse oder sogar Laufwerke zu verschlüsseln.

Weitere Tools, die auf dieser Seite angeboten werden, betreffen die Bereiche Dialer-Schutz, Browsererweiterungen, Kinderschutz, Datensicherung, Werbeschutz, Datenrettung, sichere Datenlöschung. Die wichtigsten Informationen zum Thema Datenschutz und IT-Sicherheit werden auf den Internetseiten der Staatlichen Schulämter veröffentlicht. Dort finden Sie unter dem Menüpunkt <Service> den neuen Menüpunkt <Datenschutz / IT-Sicherheit>.

Neben den relevanten Rechtsvorschriften werden dort Anleitungen zu folgenden Bereichen angeboten:

- Verschlüsselung mit TrueCrypt (Download der Software/Bedienungsanleitung). Anleitung zur Einrichtung einer Verschlüsselungsmöglichkeit auf einem externen Datenträger (z.B. USB-Stick).

- Download und Bedienungsanleitung zur Installation eines Virenschutzprogrammes.
- Download und Bedienungsanleitung zur Installation eines Programmes zum Schutz vor Spähprogrammen (adAware).
- Bedienungsanleitung zum Thema Überprüfung der Sicherheitseinstellungen (Virenschutz, Firewall etc.).
- Bedienungsanleitung zur Erstellung eines Benutzerkennwortes.

Dieses Informationsangebot zu den Bereichen Datenschutz / IT-Sicherheit wird regelmäßig aktualisiert und erweitert. Wir bitten die Lehrerinnen und Lehrer daher, diese Seiten auch regelmäßig aufzusuchen.

1.3.2 Erlass über die Information von Eltern und volljährigen Schülerinnen und Schülern über die Datenverarbeitung in der Schule

vom 19. Oktober 2009 (ABl. 2009 S. 811)

Nach der Vorgabe des Hessischen Datenschutzgesetzes sind Eltern bzw. volljährige Schülerinnen und Schüler darüber zu informieren, dass ihre Daten an der Schule gespeichert und verarbeitet werden. Dies geschieht zweckmäßigerweise bei der erstmaligen Aufnahme in eine hessische Schule.

Für diese Information steht Ihnen das als Anlage beigefügte Merkblatt zur Verfügung. Dieses übergeben Sie den Eltern bzw. volljährigen Schülerinnen und Schülern nach der Erhebung der Stammdaten. Der Ausdruck des Stammdatenblattes aus der LUSD enthält einen entsprechenden Hinweis.

Das von den Eltern bzw. Schülerinnen oder Schülern unterschriebene Merkblatt nehmen Sie bitte zu der Schülerakte.

Merkblatt

Hinweis:

Mit dem erstmaligen Besuch einer hessischen Schule wird für jede Schülerin bzw. für jeden Schüler eine Schülerakte angelegt. In dieser Akte werden zunächst die auf dem Stammblatt ausgedruckten Daten erfasst und nach und nach im Fortgang der Schullaufbahn um weitere Daten zu den besuchten Unterrichtsveranstaltungen, den Leistungen und den erreichten Abschlüssen ergänzt. Die Datenhaltung geschieht sowohl in elektronischer Form in der Lehrer- und Schülerdatenbank (LUSD) wie auch in Form einer ergänzenden Schülerakte in Papierform. Bei einem Schulwechsel werden die Schülerakte und die Zugriffsberechtigung auf die Daten auf die aufnehmende Schule übertragen.
Die Grundlage für die Datenerhebung und weitere Datenverarbeitung wird im § 83 des Hessischen Schulgesetzes und in der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 gelegt (veröffentlicht im Amtsblatt vom März 2009, im Internet siehe http://www.datenschutz.hessen.de/schuvo.htm). In dieser Verordnung finden Sie auch einen Überblick darüber, welche Daten grundsätzlich in der Schule gehalten werden dürfen und wie lange sie aufbewahrt werden müssen. Sie haben das Anrecht, nach Anmeldung die Daten bzw. die Schülerakte einzusehen. In solchen Fällen beantragten Sie dies bitte bei der Schulleitung.

Kenntnis genommen

_____

Daten / Unterschrift

(Das Merkblatt finden Sie auch als Download auf den Internetseiten der Staatlichen Schulämter unter Service/Datenschutz/IT-Sicherheit.)

1.3.3 Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen, zur Nutzung von E-Mail und zur Erhebung und Veröffentlichung interner Daten

vom 27. November 2009 – Az. 640.000.005-00002

Grundsätze

Im Rahmen der Erfüllung ihres gesetzlichen Auftrages ist die einzelne Schule veranlasst, eine Fülle von Informationen und Daten über Schülerinnen und Schülern, Lehrkräfte, Eltern aber auch über die Unterrichtsorganisation vorzuhalten, zu speichern und zu verarbeiten. Dies geschieht zunehmend nicht mehr nur in der herkömmlichen Form von Listen, Akten und Klassenbüchern, sondern auch in elektronischer Form, vor allem im Rahmen der Lehrer- und Schülerdatenbank (LUSD) oder der Nutzung elektronischer Dokumente und Tabellen. Die Rechtmäßigkeit der Haltung und Verarbeitung solcher Daten ist vor allem durch das Hessische Schulgesetz (z.B. § 83 Abs. 1 Satz 1) sowie die Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 begründet, aber auch begrenzt. Um das informationelle Selbstbestimmungsrecht der Beteiligten zu schützen, sind im Besonderen die Vorgaben des Hessischen Datenschutzgesetzes (HDSG) und hier besonders die Anforderungen an die IT-Sicherheit zu beachten. Dieser Erlass konkretisiert die Anforderungen unter besonderer Berücksichtigung der Verhältnisse in den einzelnen Schulen bzw. den Schulsekretariaten.

1. Aufklärungspflichten beim Erheben von Daten (§ 12 Abs. 4 HDSG)

Schulen erhalten die ersten personenbezogenen Daten von Schülern und Eltern bei der Erstanmeldung der Schülerin oder des Schülers an einer hessischen Schule. Soweit sie nicht aus den Systemen der Meldeämter übermittelt werden, erhebt die Schule die Daten bei Eltern und Schülern. Bei der Datenerhebung sind die Eltern bzw. die volljährigen Schüler auf die Tatsache hinzuweisen, dass diese Daten sowie weitere Daten, die im Rahmen des Schulbesuches entstehen und zur Dokumentation des Bildungsweges des Kindes notwendig sind, in der Schule gespeichert und verarbeitet werden (Aufklärungspflicht). Welche Daten dieses zunächst sind, regelt die „Verordnung zur Verarbeitung personenbezogener Daten in Schulen und Statistiken in Schulen vom 4. Februar 2009“. Darüber hinausgehende Daten können die Schulen nur verarbeiten, wenn sie bei den Betroffenen und mit deren Zustimmung und Kenntnis erhoben wurden. Diese Einwilligung bedarf der Schriftform (§ 7 Abs. 1 Nr. 3 HDSG; s. hierzu den Erlass „Information von Eltern und volljährigen Schülern über die Datenverarbeitung in der Schule, Erlass vom 19. Oktober 2009, Az. Z5 – 000.256.000-00039“).

2. Maßnahmen zum Schutz personenbezogener Daten

Es muss in der Schule sichergestellt sein, dass nur solche Personen Zugriff auf die in der Schule gespeicherten personenbezogenen Daten erhalten, bei denen für den Zugriff eine dienstliche Notwendigkeit besteht und die hierzu auch eine Befugnis haben. Dies gilt für Daten die in konventionellen Akten gehalten werden gleichermaßen wie für Zugriffe auf Daten in einem IT-Verfahren, zum Beispiel der LUSD. Dies bedeutet, dass

Lehrkräfte grundsätzlich eine Zugangsberechtigung nur zu Daten der Schüler besitzen die sie unterrichten, nicht aber zu allen Schülern der Schule. Besteht eine pädagogische Notwendigkeit, Information über andere Schüler zu erhalten, so ist das Ersuchen an den zuständigen Klassenlehrer/Klassenlehrerin oder Tutor/Tutorin oder an die Schulleitung zu richten.

3. Zuständigkeiten

Nach § 88 HSchulG ist der Schulleiter gegenüber möglichen Betroffenen, dem Hessischen Kultusministerium und dem jeweiligen Schulträger dafür verantwortlich, dass allen datenschutzrechtlichen Vorschriften Vorgaben und Notwendigkeiten Rechnung getragen wird. Diese Vorschriften verlangen vor allem folgende Maßnahmen:

- Schriftliche Bestellung des schulischen Datenschutzbeauftragten und Vertreters (§ 5 Abs. 1 HDSG und § 11 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen).
- Erstellung, Fortführung und Umsetzung eines schriftlichen IT-Sicherheitskonzeptes nach § 10 Abs. 2 Satz 2 HDSG.
- Abstimmung notwendiger Maßnahmen im Rahmen der äußeren Schulverwaltung mit dem Schulträger.

4. Technische und Organisatorische Maßnahmen

4.1 Sicherstellung ausreichender Qualifikation.
Das Personal, das für den Betrieb und die Wartung der IT in den Schulen zuständig ist, muss die ihm zu übertragenden Aufgaben fachkundig erfüllen können. Beauftragt der Schulträger eigenes oder externes Personal, so trägt er unmittelbar die Verantwortung.

4.2 Räumliche Sicherung der IT-Anlagen
Räume mit Netzstrukturen und IT-Systemen, die den Zugang auf das Verwaltungsnetz der Schulen bzw. auf das kommunale Schulträgernetz bereitstellen, unterliegen besonderen Schutzmaßnahmen, da die entsprechenden Gebäude der Öffentlichkeit während der regulären Dienstzeiten und gegebenenfalls auch zu bestimmten Anlässen auch an Wochenenden (z.B. Schulfeste oder Schule als Wahllokal) oder an Wochentagen nach der regulären Hauptarbeitszeit (z.B. Elternabende, Infoveranstaltungen etc.) zugänglich sind.

Es müssen Maßnahmen und Regelungen getroffen werden, um den unberechtigten Zutritt zu schutzbedürftigen Räumen zu verhindern:

- **Zutrittskontrolle**
  Räume, in denen PCs oder Netzwerkkomponenten des Verwaltungsnetzes stehen, sollten mit einem geeigneten Schutz gegen unbefugten Zutritt und Einbruch etc. versehen sein. Ggf. ist dieser vom Schulträger einzufordern. Der Zutritt zu Räumen mit Netzstrukturen und IT-Systemen ist ausschließlich berechtigten Personen

(Schulleitung, Lehrer, Verwaltungsangestellte, ggf. Netzwerkadministrator) gestattet. Die Räume müssen sicher verschließbar sein, der Kreis der zutrittsberechtigten Personen muss genau festgelegt werden (z.B. durch dokumentierte Schlüsselverwaltung) und die Kenntnisnahme der entsprechenden Regelungen durch die berechtigten Personen muss dokumentiert werden. Anderen Personen (z.B. Schülern etc.) ist der Zutritt allenfalls in Begleitung oder Anwesenheit berechtigter Personen erlaubt. Für Personenkreise, die außerhalb der regulären Öffnungszeiten die Räume betreten müssen (z.B. Reinigungspersonal o.Ä.) können evtl. in Absprache mit dem Schulträger Sondervereinbarung getroffen werden. Bei nicht besetzten Räumen, in denen Client-Systeme bzw. Netzinfrastruktur stehen, sind Fenster und Türen verschlossen zu halten. Schlüssel zu diesen Räumen sind nur an berechtigte Personen (kontrolliert bzw. dokumentiert) auszugeben und dürfen nicht an andere Personen weitergegeben werden (Zugangs- und Zutrittsschutz).

- **Benutzer- und Zugriffskontrolle**
  Für ein gesichertes Login an einem IT-System ist die entsprechende Authentifizierung, bestehend aus dem Benutzernamen und einem geheim zu haltenden Passwort notwendig. Regelungen zur Wahl eines sicheren Passworts sollten sich an der BSI Maßnahme M2.11 „Regelung des Passwortgebrauchs“ orientieren (Zugangs- und Zugriffsschutz). Das Passwort ist personenbezogen zu halten und in angemessenen Zeiträumen zu wechseln. Passwörter sollen mindestens acht Zeichen umfassen und möglichst eine komplexe Zusammensetzung aus Buchstaben (groß/klein), Sonderzeichen und Ziffern aufweisen. Passwörter dürfen in keinem Fall zugänglich notiert oder an andere Personen weitergegeben werden. Für Notfall-Passwörter gilt die Ausnahme, dass diese in einem Passwort-Safe hinterlegt werden dürfen.

5. Verwaltungsnetz und Verwaltungsrechner

Bei den kommenden Ausführungen wird vom (Schul-)Verwaltungsnetz und von Verwaltungsrechnern gesprochen. Verwaltungsrechner sind alle Computersysteme, die ausschließlich für Verwaltungszwecke zu nutzen sind. Eine gleichzeitige Nutzung zur Unterrichtsvorbereitung oder Ähnlichem ist nicht gestattet. Verwaltungsrechner sind entweder Stand-Alone-Geräte, die mit keinem anderen Rechner verbunden sind, sie können Geräte in einem lokalen Schulverwaltungsnetz sein und sie können darüber hinaus an das Hessische Schulverwaltungsnetz angebunden sein. In keinem Fall dürfen sie über einen ungeschützten Internetzugang verfügen. Daher bieten das Hessische Schulverwaltungsnetz bzw. die Schulnetze der Schulträger gesicherte Internetzugänge an.

Für diese Rechner gilt:

- Rechner, Datenträger und aktive Komponenten können nicht aus dem Unterrichtsbereich in den Verwaltungsbereich oder umgekehrt aus dem Verwaltungsbereich in den Unterrichtsbereich übernommen werden, ohne dass vorher vorhandene Software und Daten grundlegend gelöscht werden. Vorgehensweisen und Methoden werden im BSI Maßnahmenkatalog „M 2.167 Sicheres Löschen von Datenträgern“ beschrieben. Über das Löschen der Daten und Datenträger ist ein Vermerk zu den Akten zu nehmen.
- Entsprechend der Art des Einsatzes ist auf Schulverwaltungsrechnern auch nur solche Software einzusetzen, die zur Erfüllung dieser Aufgaben dient. Die Installation von nicht genehmigter Software (z.B. durch Downloads vom Internet oder von anderen Quellen) auf den Client-Rechnern ist nicht erlaubt und sollte nach Möglichkeit technisch unterbunden werden (Schutz vor unbeabsichtigter Installation von Schadsoftware und störende bzw. beeinträchtigende Wechselwirkungen mit benötigter Software). Die Schulträger können Genehmigungsvorbehalte zur Installation von Software erlassen. Damit soll die Verträglichkeit der Software untereinander auf den Rechnern und insbesondere die aufgabengebundene Nutzung des PCs gesichert bleiben.
- Befinden sich die Client-Systeme der Verwaltung im Verwaltungsnetz in Räumen mit Publikumsverkehr (z.B. Sekretariat oder dergleichen) ist durch eine geeignete Aufstellung der Client-Systeme (einschließlich Tastatur, Bildschirm, Drucker, Scanner und dergleichen) der Zugriff von Unbefugten zum System und die Einsichtnahme von Daten zu verhindern. Bei Abwesenheit der Zugriffsberechtigten ist das Client-System entweder ganz auszuschalten oder zu sperren. In jedem Fall muss sich spätestens nach 10 Minuten „Ruhephase“ ein mit Passwortschutz ausgestatteter Bildschirmschoner aktivieren (Zugangs- und Zugriffsschutz).
- Die Konfiguration bzw. die vorhandenen Sicherheitseinstellungen der Client-Rechner dürfen durch die Benutzer nicht verändert werden. Dies sollte nach Möglichkeit technisch unterbunden werden. Dies betrifft Soft- und Hardware. Bei entsprechenden Fragestellungen oder Problemen ist der Schulleiter und ggf. der für die Schule zuständige Support zu kontaktieren (Zugangs- und Zugriffsschutz).

6. Hardware

6.1 Schulische Netzwerke

In der Regel existieren in den Schulen Netzwerkverbindungen für Verwaltungszwecke (sog. Verwaltungsnetz) und für pädagogisch-didaktische Zwecke (sog. pädagogisches Netzwerk). Diese beiden Netzwerke sind physikalisch oder logisch strikt voneinander getrennt zu halten, da ihr Schutzbedarf jeweils unterschiedlich ist und verschiedene Zugriffsberechtigungen vorliegen können (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten).

- Eine sichere logische Trennung der Netze (z.B. durch Nutzung von VLANs auf Switches) ist technisch möglich. Die Sicherheitskonzepte zur logischen Trennung sollten die im IT-Grundschutzhandbuch des BSI im Baustein 7.11 Router „und Switches“ vorgesehenen Maßnahmen berücksichtigen und müssen dem aktuellen Stand der Technik entsprechen.

- Auf den Einsatz von WLAN sollte aus Sicherheitsgründen verzichtet werden (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten). In besonders begründeten Ausnahmefällen kann der Einsatz von WLAN auf Basis eines entsprechenden Sicherheitskonzeptes erfolgen.
- Zentrale Netzwerktechnik wie Router, Switches und Hubs soll in gesicherten, nicht öffentlich zugänglichen Räumen oder Schutzschränken untergebracht werden (s. auch Vorgaben für die IT-Infrastruktur; Zugangs- und Zutrittsschutz).
- Lehrkräfte können nur im Einvernehmen mit dem Schulträger zur Wartung der Netzwerke herangezogen werden, Schüler in keinem Fall.

6.2 Nutzung privater IT-Geräte

Private IT-Geräte dürfen grundsätzlich nicht zur Erledigung schulischer Verwaltungsarbeit benutzt werden. Eine Ausnahme bildet die Nutzung von Rechnern am häuslichen Arbeitsplatz der Lehrkräfte (s. Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft, Erlass vom 21. August 2009, Az: I.7 – 000.256.000-00027).

6.3 Mobile IT-Geräte

Mobile IT-Geräte, die in das Hessische Schulverwaltungsnetz eingebunden werden sollen, müssen ausschließlich dienstlich genutzt werden und dürfen in keiner Form anders als über das Schulverwaltungsnetz mit dem Internet verbunden werden.

6.4 Mobile Datenträger

Werden personenbezogene Daten auf mobile Datenträger ausgelagert, so ist mit entsprechender Sorgfalt zu verfahren:

- Der Datenträger mit personenbezogenen Daten ist zu registrieren.
- Soll der Datenträger auch außerhalb des Schulsekretariats bzw. der Büroräume der Schulleitung genutzt werden, so sind personenbezogene Daten zu verschlüsseln und ein gesicherter, überwachter Transport zu gewährleisten. Bei Daten die aus der LUSD geliefert werden (Externer Notenerfassungs-Client) wird diese Verschlüsselung automatisch hergestellt.
- Dienstlich gestellte Datenträger dürfen grundsätzlich nur für dienstliche Zwecke und zum Datentransport zwischen Verwaltungsrechnern verwendet werden.
- Werden die auf mobilen Datenträgern gespeicherten Daten nicht mehr benötigt, sind sie in das zentrale System zurückzuspielen und auf dem mobilen Datenträger zu löschen. Die Schulen und Schulträger können für die Nutzung mobiler Datenträger Richtlinien erlassen oder eine spezielle Schutzsoftware zur technischen Registrierung von externen Datenträgern einsetzen. Andere, nicht registrierte Datenträger können dann an den Verwaltungsrechnern nur noch nach gesonderter Freigabe verwendet werden.

7. Schutz vor Schadprogrammen

In den dezentralen Netzen liegt die Verantwortung für einen funktionsfähigen und stets aktuellen Schutz vor Schadprogrammen beim Schulleiter und Schulträger gleichermaßen. Zu den Aufgaben der Schulleitung gehören unter anderem

- die Sensibilisierung der Nutzer für vorhandene Gefahren durch Viren,
- die Information der Nutzer über Vorsichtsmaßnahmen und Verhaltensregeln zum Schutz vor Viren,
- dafür zu sorgen, dass geeignete Virenschutzmaßnahmen auf gefährdeten IT-Systemen implementiert werden,
- das Aufstellen von Verhaltensregeln für einen eingetretenen oder vermuteten Virenbefall, z.B. Benachrichtigung einer Hotline oder des IT-Supports, um eine Beseitigung der Virusinfektion zu veranlassen und sofortiges Einstellen der Arbeit am befallenen Client-Rechner.

8. Konventionelle und elektronische Datenspeicherung und Datensicherung

8.1 Aufbewahrung von Schülerakten

Die Schülerakten, Karteikarten mit personenbezogenen Angaben, entsprechende Listen etc. sind grundsätzlich nur in ausreichend sicheren Schränken zu verwahren (Stahlschrank mit Sicherheitsschloss o.Ä.). Bei größeren Schulsystemen empfiehlt es sich, die Akten stufen- oder zweigweise gegliedert in unterschiedlichen Schränken aufzubewahren, so dass dann, wenn ein Zugang notwendig wird, nie der gesamte Aktenbestand angeboten werden muss.

8.2 Elektronische Speicherung

Werden über die Nutzung der LUSD hinaus in der Schule elektronische Dokumente auf Verwaltungsrechnern gespeichert, so ist dafür – ggf. in Absprache mit dem Schulträger – ein entsprechendes Dateiablage-Konzept zu entwickeln. Handelt es sich um Dateien mit personenbezogenen Inhalten, muss der Zugang zu den entsprechenden Ablagesegmenten ausreichend geschützt werden, handelt es sich dabei auch um Daten nach § 7 Abs. 4 HDSG, sind diese Daten zwingend verschlüsselt abzulegen.

8.3 Datensicherung

Zur Gewährleistung von Datenschutz und IT-Sicherheit gehört auch, dass die Verfügbarkeit der Daten gesichert ist. Für die Daten der LUSD übernimmt dies die Hessische Zentrale für Datenverarbeitung, dort ist ein entsprechendes Datensicherungssystem aktiv.

- Für darüber hinaus auf Verwaltungsrechnern/Servern der Schule gehaltene Daten hat die Schulleitung für eine entsprechende Datensicherung zu sorgen. Diese hat regelmäßig und in ausreichender Frequenz zu erfolgen (Tages-, Wochen- und Monatssicherung).

- Die Datenträger, auf denen diese Datensicherung erfolgt sind entsprechend der Sensibilität der jeweiligen Dateien geschützt aufzubewahren. Dies bedeutet nicht nur den Schutz vor unbefugten Zugriffen, sondern auch vor Beschädigung durch Feuer, Wasser oder Diebstahl. Daher sind sie nicht im gleichen Raum wie Rechner oder Server aufzubewahren, sondern in einem anderen Raum, möglichst in einem anderen Gebäude(teil).
- Existiert an der Schule ein Client-Server-System, so sind die Daten grundsätzlich auf dem Server zu speichern. Die Daten auf dem Server sind zentral zu sichern und die Datenträger vorzugsweise in separaten Räumlichkeiten zu verwahren. Zusätzliche lokale Speicherung personenbezogener Daten auf den Clients hat zu unterbleiben.

9. Elektronischer Mailverkehr

9.1 Postfächer

Mit der Einrichtung des Hessischen Schulnetzes erhielten alle beteiligten hessischen Schulen drei Funktionspostfächer:

- Das Funktionspostfach „Poststelle“
- Das Funktionspostfach „Schulleitung“
- Das Funktionspostfach „Landesaufgaben“

Darüber hinaus konnten personalisierte Postfächer zur Verfügung gestellt werden. In einzelnen Schulträgerbereichen mit eigenen Netzen werden schulträgerspezifische Postfächer genutzt, die ebenfalls an das Schulverwaltungsnetz angebunden sind.

Das Funktionspostfach „Poststelle“ ist als offizielle Mailadresse der Schule zu verwenden. Es fungiert zugleich als elektronische Posteingangsstelle. Die Verwendung der anderen Funktionspostfächer ergibt sich aus ihrer Bezeichnung. Eine Vertretungsregelung hat sicherzustellen, dass eingehende Mail geöffnet und bearbeitet werden kann. Dies kann erfolgen durch Weiterleitung der Posteingänge oder durch Zugriffsgewährung auf das E-Mail-Postfach.

Achtung: Von den im Schulnetz eingerichteten Postfächern darf keine automatisierte Weiterleitung der Mails an private Postfächer außerhalb des Schulverwaltungsnetzes erfolgen (vgl. dazu Abschnitt **Mail-Umleitung**).

9.2 Allgemeine Grundsätze der Nutzung

Die dienstliche Mailadresse ist nur für dienstliche Zwecke zu nutzen. Grundsätzlich sollen im innerbehördlichen Schriftverkehr alle Schreiben und sonstige Dokumente per E-Mail versandt werden, die nicht eine persönliche Unterschrift erfordern oder vertraulich zu behandelnde Daten enthalten.

9.3 Mail-Eingang

Die elektronischen Informationen (Mails) sind in geeigneter Weise in den Geschäftsgang zu bringen und, soweit sie für den Nachweis des Standes und der Entwicklung der

Vorgangsbearbeitung nicht offenkundig unerheblich sind, elektronisch oder in Papierform (als Ausdruck) zu den Akten zu nehmen (siehe „Archivierung“).

9.4 Mail-Ausgang

Bei der Nutzung der E-Mail ist zunächst zu unterscheiden, ob es sich um allgemeine Nachrichten, Terminabsprachen o.Ä. handelt oder ob ein Dokument mit Aktenrelevanz versandt werden soll. Die folgenden Regelungen beziehen sich auf die letztgenannten Dokumente.

Der elektronische Versand in Form einer einfachen E-Mail (unverschlüsselt und unsigniert) eignet sich nicht, soweit höherwertige Formvorschriften (z.B. handschriftliche Unterschrift, Urkundenform) bestehen. Für einen Versand per E-Mail sind die einschlägigen gesetzlichen Bestimmungen zum Ersatz dieser Formen in elektronischen Dokumenten zu beachten.

Werden keine Verschlüsselungsverfahren angewendet und erfolgt der Versand nicht oder nicht ausschließlich im Schulnetz, sondern im Internet, entsprechen E-Mails einer „offenen Postkarte“. Die Übermittlung von vertraulich zu behandelnder Informationen oder schutzwürdiger personenbezogenen Daten darf daher auf elektronischem Weg nur bei Nutzung einer den BSI-Standards entsprechenden Verschlüsselung erfolgen.

Im elektronischen Dokument genügt an Stelle der Unterschrift der Vermerk „gez.“ In Verbindung mit dem Namen der unterzeichnenden Person und der Fixierung des Datums. Ein Bestätigungsvermerk entfällt. Ausgehenden E-Mails, die auch in Papierform vorhanden sind, liegt ein abgezeichneter Entwurf zu Grunde. Der Versand ist durch handschriftlichen Vermerk oder Versandprotokoll aktenkundig zu machen.

9.5 Mail-Umleitung

Eine Umleitung von Mails auf Postfächer im Internet birgt immer die Gefahr, dass Mails von nicht berechtigten Personen gelesen und auch verändert werden können. Daher gilt:

- Für das Postfach „Landesaufgaben“ ist keine Form der Umleitung zulässig.
- Eine automatisierte Umleitung darf im Übrigen nur auf solche Postfächer eingerichtet werden, die sich im Schulnetz oder einem entsprechend abgesicherten Netz des Schulträgers befinden.
- Eine automatisierte Umleitung in das sichere Netz des Schulträgers erfordert die Zustimmung und Absprache zwischen Schulträger und HKM.
- Eine manuelle Umleitung auf Postfächer im Internet ist nur im Einzelfall zulässig und auch nur dann, wenn geprüft wurde, dass die Mail keine vertraulichen oder personenbezogenen Daten enthält.

Es ist grundsätzlich zu beachten, dass bei umgeleiteten Mails und der Nutzung der „Antworten-Funktion“ als Absenderangabe nicht mehr die offizielle Schuladresse erscheint.

9.6 Archivierung

Da die Kapazitäten der Postfächer beschränkt sind, sind diese immer wieder rechtzeitig zu sichten. Aktenrelevante Mails sind als Ausdruck den Akten beizufügen, oder - wenn ein elektronisches Dokumentenmanagementsystem vorhanden ist - dort abzuspeichern und zu archivieren. Das Mailsystem ersetzt keine Ablage. Danach sind die Mails zu löschen.

Die übrige Post ist nach angemessener Frist zu löschen.

9.7 Geschützte Dokumente und Anlagen

Es ist notwendig, Dokumente, die man vor Veränderungen schützen will, im pdf-Format zu versenden. Dieses Format erfordert in der Regel auch weniger Speicherplatz. Versendet man mit der Mail Dokumente als Anhang, so ist auf deren Größe zu achten, vor allem, wenn ein großer Adressatenkreis erreicht werden soll. Ausführbare Dateien (Endungen wie exe oder mdb) werden vom System aus Sicherheitsgründen gesperrt.

10. Erhebung und Veröffentlichung von Daten

Für die Erhebung von nicht personenbezogenen Daten im Zuständigkeitsbereich des Hessischen Kultusministeriums wird vorzugsweise das Verfahren ESDAL (**E**rhebung **S**tatistischer **DA**ten im **L**andesschulnetz) eingesetzt. Das Verfahren bietet die Vorteile einer einfachen Bedienung über eine Browser-Oberfläche, einer sicheren Datenübermittlung aus dem Landesschulnetz in das Landesverwaltungsnetz und der Nutzung der vorhandenen Benutzerkonten des Verfahrens LUSD. Eine gesonderte Benutzerkontenverwaltung für die Schulen, wie sie bei der Erhebung von Daten über das Internet üblicherweise erforderlich ist, kann somit entfallen. Es entfällt ebenfalls der Versand von Dateien mit Erfassungsdaten als E-Mail-Anhang, womit die Zuverlässigkeit und Sicherheit der Datenübermittlung verbessert wird.

Die Publikation von Statistischen Berichten aus dem Landesverwaltungsnetz in das Landesschulnetz erfolgt vorzugsweise über das Verfahren ISIS (**I**nformations**S**ystem **I**m **S**chulnetz). Das Verfahren erlaubt die schulbezogene Veröffentlichung von Berichten in unterschiedlichen technischen Formaten im Landesschulnetz. Über die Nutzung des Berechtigungssystems der LUSD wird sichergestellt, dass Zugriff auf den Bericht über eine Schule nur die jeweilige Schule und das Aufsicht führende Staatliche Schulamt haben.

11. Aufhebung von Erlassen

Die Richtlinie zur Nutzung des Hessischen Schulnetzes und zum Umgang mit E-Mail, Erlass vom 8. August 2007, Az. I.7 – 640.000.010-46 wird aufgehoben.

2. Hessisches Datenschutzgesetz (HDSG)

in der Fassung vom 7. Januar 1999 (GVBl. I S. 98)

Inhaltsübersicht

DRITTER TEIL
Besonderer Datenschutz

VIERTER TEIL
Rechte des Landtags und der kommunalen Vertretungsorgane

FÜNFTER TEIL
Schlussvorschriften

ERSTER TEIL
Allgemeiner Datenschutz

ERSTER ABSCHNITT
Grundsatzregelungen

§ 1
Aufgabe

(1) Aufgabe des Gesetzes ist es, die Verarbeitung personenbezogener Daten durch die in § 3 Abs. 1 genannten Stellen zu regeln, um

1. das Recht des Einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind,
2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Aufgabe der obersten Landesbehörden, Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts ist es, die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz jeweils für ihren Bereich sicherzustellen.

§ 2
Begriffsbestimmungen

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

(2) Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist

1. Erheben das Beschaffen von Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die Daten verarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft,
4. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,
5. Löschen das Unkenntlichmachen gespeicherter Daten

ungeachtet der dabei angewendeten Verfahren.

(3) Daten verarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

(4) Empfänger ist jede Person oder Stelle, die Daten erhält.

(5) Dritter ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie Daten im Auftrag verarbeiten.

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

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

(8) Soweit andere landesrechtliche Vorschriften den Dateibegriff verwenden, ist Datei

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder
2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei).

§ 3
Anwendungsbereich

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen ungeachtet ihrer Rechtsform. Dieses Gesetz gilt auch für nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der in Satz 1 genannten Stellen wahrnehmen.

(2) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(3) Soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

(4) Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

(5) Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet, gelten von den Vorschriften

dieses Gesetzes nur die §§ 10 und 37. Im Übrigen gelten die Vorschriften dieses Gesetzes.

(6) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie die §§ 34 und 36 dieses Gesetzes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im Übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

§ 4
Verarbeitung personenbezogener Daten im Auftrag

(1) Die Daten verarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie für die Erfüllung ihrer sich aus § 8 ergebenden Pflichten auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

(4) Abs. 1 bis 3 gelten auch für Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Datenverarbeitung erledigen.

§ 5
Behördlicher Datenschutzbeauftragter

(1) Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muss der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Wegen dieser Tätigkeit, bei der er frei von Weisungen ist, darf er nicht benachteiligt werden. Er ist insoweit unmittelbar der Leitung der Daten verarbeitenden Stelle zu unterstellen; in Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. Der behördliche Datenschutzbeauftragte ist im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen sowie mit den zur Erfüllung seiner Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten. Die Beschäftigten der Daten verarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

(2) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 geschützte Recht betreffen, hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 erforderlichen Maßnahmen zu unterstützen,
4. das nach § 6 Abs. 1 zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Abs. 2 bereitzuhalten,
5. das Ergebnis der Untersuchung nach § 7 Abs. 6 zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten und die automatisierte Datenverarbeitung nehmen. Vor einer beabsichtigten Maßnahme nach Satz 2 Nr. 1 ist er rechtzeitig umfassend zu unterrichten und anzuhören. Wird er nicht rechtzeitig an einer Maßnahme beteiligt, ist die Entscheidung über die Maßnahme auszusetzen und die Beteiligung nachzuholen.

(3) Die Daten verarbeitende Stelle kann einen Beschäftigten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere Daten verarbeitende Stellen können gemeinsam einen ihrer Beschäftigten zum Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird. Bestellungen von Personen, die nicht der Daten verarbeitenden Stelle angehören, sind dem Hessischen Datenschutzbeauftragten mitzuteilen.

§ 6[1]
Verfahrensverzeichnis

(1) Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der Daten verarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens,
9. Fristen für die Löschung nach § 19 Abs. 3,
10. eine beabsichtigte Datenübermittlung nach § 17 Abs. 2,
11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.

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

Satz 1 gilt nicht für

1. Verfahren des Landesamtes für Verfassungsschutz,
2. Verfahren, die der Gefahrenabwehr oder der Strafverfolgung dienen,
3. Verfahren der Steuerfahndung,

soweit die Daten verarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

§ 7
Zulässigkeit der Datenverarbeitung

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

1. eine diesem Gesetz vorgehende Rechtsvorschrift sie vorsieht oder zwingend voraussetzt,
2. dieses Gesetz sie zulässt oder
3. der Betroffene ohne jeden Zweifel eingewilligt hat.

(2) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sie muss sich im Falle einer Datenverarbeitung nach

[1] § 6 tritt am 1. Juni 1999 in Kraft.

Abs. 4 ausdrücklich auch auf die dort genannten Daten beziehen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) Unzulässig ist eine zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führende Entscheidung, wenn sie auf einer Bewertung einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, das die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

(4) Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im Übrigen ist eine Verarbeitung auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.

(5) Wenn der Betroffene schriftlich begründet, dass der rechtmäßigen Verarbeitung seiner Daten auf Grund dieses Gesetzes schutzwürdige, sich aus seiner besonderen persönlichen Lage ergebende Gründe entgegenstehen, ist die Verarbeitung nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, dass seine Gründe hinter dem öffentlichen Interesse an der Verarbeitung zurückstehen müssen. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen.

(6) Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

(7) Die in § 3 Abs. 1 Satz 2 und Abs. 6 genannten Stellen dürfen Daten, die Straftaten betreffen, nur unter behördlicher Aufsicht verarbeiten oder wenn eine Rechtsvorschrift dies vorsieht.

§ 8
Rechte der Betroffenen

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten (§ 18),
2. Überprüfung der rechtmäßigen Verarbeitung seiner Daten auf Grund von ihm vorgebrachter besonderer persönlicher Gründe (§ 7 Abs. 5),
3. Einsicht in das Verfahrensverzeichnis (§ 6 Abs. 2),
4. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 19),
5. Schadensersatz (§ 20),
6. Anrufung des Datenschutzbeauftragten (§§ 28 und 37 Abs. 2).

(2) Wenn eine in § 3 Abs. 1 genannte Stelle für die Gewährung einer Leistung, das Erkennen einer Person oder für einen anderen Zweck einen Datenträger herausgibt, auf dem personenbezogene Daten des Inhabers automatisiert verarbeitet werden, etwa in Form einer Chipkarte verarbeitet werden, dann hat sie sicherzustellen, dass er dies erkennen und seine ihm nach Abs. 1 Nr. 1 bis 5 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe des Datenträgers über die ihm nach Abs. 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

§ 9
Datengeheimnis

Den bei der Daten verarbeitenden Stelle oder in deren Auftrag beschäftigten Personen, die Zugang zu personenbezogenen Daten haben, ist eine Verarbeitung dieser Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck während und nach Beendigung ihrer Tätigkeit untersagt. Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 10
Technische und organisatorische Maßnahmen

(1) Die Daten verarbeitende oder in ihrem Auftrag tätige Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die nach Abs. 2 und 3 erforderlich sind, um die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu gewährleisten. Erforderlich sind diese Maßnahmen, soweit der damit verbundene Aufwand unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Verarbeitung zum Schutz des in § 1 Abs. 1 Nr. 1 genannten Rechts angemessen ist.

(2) Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der

Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass

1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zutrittskontrolle),
2. Unbefugte an der Benutzung von Datenverarbeitungsanlagen und -verfahren gehindert werden (Benutzerkontrolle),
3. die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),
5. es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle),
6. personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist (Dokumentationskontrolle),
8. die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

ZWEITER ABSCHNITT
Rechtsgrundlage der Datenverarbeitung

§ 11
Erforderlichkeit

(1) Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss bei einer der beteiligten Stellen vorliegen.

(2) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßíg großem Aufwand möglich ist, dann sind die Kenntnisnahme, die Weitergabe innerhalb der Daten verarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung

der jeweiligen Aufgabe erforderlich sind, über Abs. 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

§ 12
Erheben

(1) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmbaren Personenkreis, etwa durch Videoüberwachung, erhoben, dann genügt es, wenn er die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme hat.

(2) Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder der Betroffene eingewilligt hat,
2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen; der Betroffenen ist darauf hinzuweisen, bei welchen Personen oder Stellen seine Daten erhoben werden können,
3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit dies gebietet,
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(3) Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt.

(4) Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, dann ist er von der Daten verarbeitenden Stelle in geeigneter Weise über deren Anschrift, den Zweck der Datenerhebung sowie über seine Rechte nach § 8 aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Im Übrigen ist er darauf hinzuweisen, dass er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

(5) Werden Daten beim Betroffenen ohne seine Kenntnis erhoben, dann ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr

gefährdet wird. Die Benachrichtigung umfasst die Angabe der Rechtsgrundlage und die in Abs. 4 Satz 1 und 2 vorgesehene Aufklärung.

§ 13
Zweckbindung

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

(3) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe von Abs. 2 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(4) Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken in dem dafür erforderlichen Umfang verwendet werden.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

§ 14
Verantwortlichkeit für die Zulässigkeit der Datenübermittlung

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben eines in § 3 Abs. 1 genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

§ 15
Gemeinsame Verfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das mehreren Daten verarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Benutzung des Verfahrens ist im Einzelfall nur erlaubt, wenn hierfür die Zulässigkeit der Datenverarbeitung gegeben ist. Vor der Einrichtung oder Änderung eines gemeinsamen Verfahrens ist der Hessische Datenschutzbeauftragte zu hören. Ihm sind die Festlegungen nach Abs. 2 Satz 1, das Verfahrensverzeichnis nach § 6 Abs. 1 und das Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3 vorzulegen.

(2) Die beteiligten Stellen bestimmen eine Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt und legen schriftlich fest

1. die Bezeichnung und die Aufgaben jeder beteiligten Daten verarbeitenden Stelle sowie den Bereich der Datenverarbeitung, für deren Rechtmäßigkeit sie im Einzelfall verantwortlich ist und
2. die für die Durchführung des gemeinsamen Verfahrens nach § 10 Abs. 2 getroffenen technischen und organisatorischen Maßnahmen.

Die mit der Durchführung des gemeinsamen Verfahrens betraute Stelle verwahrt ein Doppel des von den beteiligten Stellen nach § 6 Abs. 1 zu erstellenden Verfahrensverzeichnisses und hält es zusammen mit den Angaben nach Satz 1 Nr. 1 zur Einsicht für die Öffentlichkeit bereit; dies gilt auch für die Angaben nach Satz 1 Nr. 2, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. § 6 Abs. 2 gilt entsprechend.

(3) Stellen, auf die dieses Gesetz keine Anwendung findet, können am gemeinsamen Verfahren beteiligt werden, wenn vertraglich sichergestellt ist, dass sie in diesem Verfahren die Bestimmungen dieses Gesetzes beachten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen.

(4) Die Betroffenen können ihre Rechte nach § 8 Abs. 1 Nr. 1 bis 5 gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der betroffenen Daten verantwortlich ist. Die Stelle, an die der Betroffene sich wendet, leitet das Anliegen an die jeweils zuständige Stelle weiter. Das Auskunftsrecht nach § 18 erstreckt sich auch auf die Angaben nach Abs. 2 Satz 1 Nr. 1.

(5) Die Abs. 1, 2 und 4 Satz 3 gelten entsprechend, wenn innerhalb einer Daten verarbeitenden Stelle ein gemeinsames automatisiertes Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

§ 16
Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist über §§ 11 und 13 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht

und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

§ 17
Übermittlung an Empfänger außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Zulässigkeit der Übermittlung personenbezogener Daten innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie gelten die Vorschriften dieses Gesetzes.

(2) Eine Übermittlung an Empfänger außerhalb des in Abs. 1 genannten Bereichs ist auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessener Datenschutz gewährleistet ist. Vor der Entscheidung über die Angemessenheit ist der Hessische Datenschutzbeauftragte zu hören. Sofern beim Empfänger kein angemessener Datenschutz gewährleistet ist, dürfen personenbezogene Daten nur übermittelt werden, wenn

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
4. 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 offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Der Empfänger, an den die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken zu vereinbaren sind, zu deren Erfüllung sie ihm übermittelt werden.

DRITTER ABSCHNITT
Rechte des Betroffenen

§ 18
Auskunft und Benachrichtigung

(1) Daten verarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben die Betroffenen von dieser Tatsache schriftlich zu benachrichtigen und dabei die Art der Daten sowie die Zweckbestimmung und die Rechtsgrundlage der Speicherung zu nennen. Die Benachrichtigung erfolgt zum Zeitpunkt der Speicherung oder im Fall

einer beabsichtigten Übermittlung spätestens mit deren Durchführung. Dienen die Daten der Erstellung einer beabsichtigten Mitteilung an den Betroffenen, kann die Benachrichtigung mit dieser Mitteilung verbunden werden.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. die Daten beim Betroffenen erhoben oder von ihm mitgeteilt worden sind,
2. die Verarbeitung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist,
3. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt hat,
4. die Benachrichtigung des Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

(3) Daten verarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger übermittelter Daten, soweit dies gespeichert ist.

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

(4) Abs. 1 und 3 gelten nicht für personenbezogene Daten, die deshalb gesperrt sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sowie für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

(5) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

(6) Abs. 1 und 3 gelten nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft der Leiter der speichernden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass er sich an den Hessischen Datenschutzbeauftragten wenden kann.

(7) Bei Prüfungs- und Berufungsverfahren können die in Abs. 1 bis 6 gewährten Rechte erst nach dem Verfahrensabschluss geltend gemacht werden.

§ 19
Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
2. ihre Verarbeitung unzulässig ist und die Löschung den Betroffenen in der Verfolgung seiner Rechte beeinträchtigen würde.

Bei automatisierten Verfahren ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im Übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr verarbeitet werden, es sei denn, dass die Verarbeitung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im rechtlichen Interesse eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene in die Verarbeitung eingewilligt hat.

(3) Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(4) Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist.

(5) Empfänger personenbezogener Daten sind unverzüglich von der Berichtigung nach Abs. 1 sowie von der Sperrung nach Abs. 2 und der Löschung nach Abs. 4 zu unterrichten. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(6) Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Abs. 3 nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist. Die Abs. 1 bis 4 gelten nicht für Stellen, die Akten nur vorübergehend beigezogen haben.

§ 20

Schadensersatz

(1) Wird der Betroffene durch eine unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten in seinen Rechten nach § 1 Abs. 1 Nr. 1 beeinträchtigt, so hat ihm der Träger der Daten verarbeitenden Stelle den daraus entstehenden Schaden zu ersetzen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von fünfhunderttausend Deutsche Mark.

(2) Auf das Mitverschulden des Betroffenen und auf die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(3) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(4) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

ZWEITER TEIL
Hessischer Datenschutzbeauftragter

§ 21
Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung den Hessischen Datenschutzbeauftragten.

(2) Der Präsident des Landtags verpflichtet den Hessischen Datenschutzbeauftragten vor dem Landtag, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren.

(3) Der Hessische Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis. Das Amt kann auch einem Beamten im Nebenamt, einem beurlaubten Beamten oder einem Ruhestandsbeamten übertragen werden.

(4) Der Hessische Datenschutzbeauftragte wird für die Dauer der jeweiligen Wahlperiode des Landtags gewählt; nach dem Ende der Wahlperiode bleibt er bis zur Neuwahl im Amt. Die Wiederwahl ist zulässig. Vor Ablauf der Amtszeit kann er nur abberufen werden, wenn Tatsachen vorliegen, die bei einem Beamten die Entlassung aus dem Dienst rechtfertigen. Er kann jederzeit von seinem Amt zurücktreten. Er bestellt für den Fall seiner Verhinderung oder für den Fall seines vorzeitigen Ausscheidens aus dem Amt für die Zeit bis zur Wahl seines Nachfolgers einen Beschäftigten seiner Dienststelle zum Vertreter. Als Verhinderung gilt auch, wenn im Einzelfall in der Person des Hessischen Datenschutzbeauftragten Gründe vorliegen, die bei einem Richter zum Ausschluss von der Mitwirkung oder zur Ablehnung wegen Besorgnis der Befangenheit

führen können.

(5) Der Hessische Datenschutzbeauftragte kann an den Sitzungen des Landtags und seiner Ausschüsse nach Maßgabe der Geschäftsordnung des Landtags teilnehmen und sich zu Fragen äußern, die für den Datenschutz von Bedeutung sind.

(6) Die Vergütung des Hessischen Datenschutzbeauftragten ist durch Vertrag zu regeln.

§ 22
Unabhängigkeit

Der Hessische Datenschutzbeauftragte ist als oberste Landesbehörde in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen.

§ 23
Verschwiegenheitspflicht

Der Hessische Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Hessische Datenschutzbeauftragte gilt als oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung. Er entscheidet entsprechend nach den Bestimmungen über die Vorlage- und Auskunftspflichten von Behörden in den gerichtlichen Verfahrensordnungen. Er trifft die Entscheidungen nach §§ 75 und 76 des Hessischen Beamtengesetzes für sich und die ihm zugewiesenen Bediensteten in eigener Verantwortung.

§ 24
Aufgaben

(1) Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Daten verarbeitenden Stellen. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen Daten verarbeitenden Stellen in Fragen des Datenschutzes beraten. Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich und soweit sie sich nach § 4 Abs. 3 Satz 1 seiner Kontrolle unterworfen haben.

(2) Der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die

Entscheidungsbefugnisse der Daten verarbeitenden Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(3) Der Hessische Datenschutzbeauftragte arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, zusammen.

(4) Zum Zwecke der Zusammenarbeit kann der Hessische Datenschutzbeauftragte von den nach den Vorschriften des Bundesdatenschutzgesetzes in Hessen für nicht-öffentliche Stellen zuständigen Aufsichtsbehörden Auskünfte verlangen. Bei der Überprüfung nicht-öffentlicher Stellen kann er mit seiner Zustimmung beteiligt werden. Gibt er der zuständigen Aufsichtsbehörde Verstöße gegen Datenschutzvorschriften bei nicht-öffentlichen Stellen bekannt, unterrichtet ihn die Aufsichtsbehörde von Zeitpunkt, Umfang und Ergebnis der Überprüfung.

§ 25
Gutachten und Untersuchungen

(1) Der Landtag und die Landesregierung können den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen und Fragen des freien Zugangs zu Informationen betrauen.

(2) Der Landtag, der Präsident des Landtags und die in § 38 Abs. 3 genannten Vertretungsorgane können verlangen, dass der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nicht oder nicht ausreichend beantwortet wurden.

§ 26
Frist

Soweit der Hessische Datenschutzbeauftragte auf Grund einer Rechtsvorschrift gehört wird, teilt er unverzüglich mit, ob und innerhalb welcher Frist er eine Stellungnahme abgeben wird.

§ 27
Beanstandungen durch den Hessischen Datenschutzbeauftragten

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Hessische 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) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

§ 28
Anrufung des Hessischen Datenschutzbeauftragten

(1) Jeder kann sich an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch Daten verarbeitende Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein. Niemand darf dafür gemaßregelt oder benachteiligt werden, dass er sich auf Grund tatsächlicher Anhaltspunkte für einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz an den Hessischen Datenschutzbeauftragten wendet.

(2) Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten wenden. Die dienstrechtlichen Pflichten der Beschäftigten bleiben im Übrigen unberührt.

§ 29
Auskunftsrecht des Hessischen Datenschutzbeauftragten

(1) Alle Daten verarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. Zutritt zu allen Diensträumen zu gewähren.

(2) Die Rechte nach Abs. 1 dürfen nur vom Hessischen Datenschutzbeauftragten persönlich ausgeübt werden, wenn die oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet. In diesem Fall müssen personenbezogene Daten eines Betroffenen, dem von der Daten verarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihm gegenüber nicht offenbart werden.

(3) Der Hessische Datenschutzbeauftragte ist über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu unterrichten.

§ 30
Berichtspflicht

(1) Zum 31. Dezember jeden Jahres hat der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 10 und regt Verbesserungen des Datenschutzes an. Zwischenberichte sind zulässig.

(2) Die Landesregierung legt ihre Stellungnahme zu dem Haupt- oder Zwischenbericht dem Landtag vor. Zusammen mit der Stellungnahme zum Hauptbericht gibt sie einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden.

§ 31
Personal- und Sachausstattung

(1) Dem Hessischen Datenschutzbeauftragten ist vom Präsidenten des Landtags die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen.

(2) Die Beamten werden auf Vorschlag des Hessischen Datenschutzbeauftragten ernannt. Ihr Dienstvorgesetzter ist der Hessische Datenschutzbeauftragte, an dessen Weisungen sie ausschließlich gebunden sind. Für sonstige Beschäftigte gelten Satz 1 und 2 entsprechend.

DRITTER TEIL
Besonderer Datenschutz

§ 32
Datenverarbeitung für Planungszwecke

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten gesondert verarbeitet werden. Die Verarbeitung soll von der übrigen Verwaltung personell und organisatorisch getrennt erfolgen.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, dass sie sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

§ 33
Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen Daten verarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen im Rahmen bestimmter Forschungsvorhaben verarbeiten, soweit dessen schutzwürdige Belange wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Im Falle des Satz 2 bedarf die Verarbeitung durch Stellen des Landes der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

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

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Abs. 2 und 3 einzuhalten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

§ 34
Datenschutz bei Dienst- und Arbeitsverhältnissen

(1) Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(3) Das Auskunftsrecht nach § 18 Abs. 3 umfasst auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 6 findet keine Anwendung.

(4) Im Falle des § 19 Abs. 3 Satz 1 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Vor Einführung, Anwendung, Änderung oder Erweiterung eines automatisierten Verfahrens zur Verarbeitung von Daten der Beschäftigten hat die Dienststelle das Verfahrensverzeichnis (§ 6) der Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens mit dem Hinweis vorzulegen, dass sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann. Macht die Personalvertretung von dieser Möglichkeit Gebrauch, beginnt die von ihr einzuhaltende Frist erst mit der Vorlage der von der Dienststellenleitung einzuholenden Stellungnahme.

(6) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 35
Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Übermittlung an öffentliche Stellen nur zulässig, sofern sichergestellt ist, dass bei dem Empfänger gleichwertige Datenschutzmaßnahmen getroffen werden.

§ 36
Fernmessen und Fernwirken

Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

§ 37
Datenverarbeitung des Hessischen Rundfunks zu journalistisch-redaktionellen Zwecken

(1) Führt die journalistisch-redaktionelle Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Der Rundfunkrat bestellt einen Beauftragten für den Datenschutz, der die Ausführung von Abs. 1 und § 10 sowie anderer Vorschriften über den Datenschutz im journalistisch-redaktionellen Bereich frei von Weisungen überwacht. An ihn kann sich jedermann wenden, wenn er annimmt, bei der Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken in seinen Rechten verletzt worden zu sein. Beanstandungen richtet der Beauftragte für den Datenschutz an den Intendanten und unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

(3) Dem nach Abs. 2 zu bestellenden Beauftragten für den Datenschutz können auch die Aufgaben nach § 5 zugewiesen werden.

VIERTER TEIL
Rechte des Landtags und der kommunalen Vertretungsorgane

§ 38
Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, dem Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeit verlangten Auskünfte auf Grund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse

nicht entgegenstehen; dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff zu den Daten, soweit durch technische Maßnahmen sichergestellt ist, dass die Grenzen der Sätze 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden Verfahren verlangen, die für Auskünfte oder den Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf

1. den Namen des Verfahrens mit kurzer Funktionsbeschreibung,
2. die vorhandenen Verfahren,
3. den Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,
4. die vorhandenen Auswertungsprogramme,
5. die zuständige Behörde.

(3) Das Auskunftsrecht nach Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen anderer in § 3 Abs. 1 genannten Körperschaften und Anstalten gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Gemeindeverbände zu, die Datenverarbeitungsanlagen betreiben. Der Antrag der Fraktionen ist in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuss zu leiten.

§ 39
Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane

(1) Mit Ausnahme der §§ 1 Abs. 1 Nr. 2, 25 und 38 gelten die Vorschriften dieses Gesetzes für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird, insbesondere wenn es sich um die wirtschaftlichen Angelegenheiten des Landtags, die Personalverwaltung oder die Ausführung von gesetzlichen Vorschriften, deren Vollzug dem Präsidenten des Landtags zugewiesen ist, handelt. Im Übrigen gibt sich der Landtag unter Berücksichtigung seiner verfassungsrechtlichen Stellung eine Datenschutzordnung. Sie findet auf die für die Fraktionen und Abgeordneten tätigen Personen entsprechende Anwendung.

(2) Die Landesregierung darf personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten im Rahmen der Geschäftsordnung des Hessischen Landtags in dem dafür erforderlichen Umfang verwenden. Dies gilt nicht, wenn die Übermittlung der Daten wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

(3) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise allgemein zugänglich

gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden.

(4) Abs. 2 gilt entsprechend für die Verwaltungsbehörden der Gemeinden und Gemeindeverbände im Rahmen ihrer jeweiligen Auskunftspflichten nach der Hessischen Gemeindeordnung und der Hessischen Landkreisordnung.

FÜNFTER TEIL
Schlussvorschriften

§ 40
Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten entgegen den Vorschriften dieses Gesetzes

1. erhebt, speichert, zweckwidrig verwendet, verändert, übermittelt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder einen Dritten veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

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

§ 41
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen § 16 Abs. 2 oder § 33 Abs. 3 Daten nicht nur für den Zweck verwendet, zu dessen Erfüllung sie ihm übermittelt wurden.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

§ 42
Übergangsvorschrift

Auf Akten, die bei Inkrafttreten des Gesetzes vorhanden waren, ist § 19 Abs. 1, 4 und 6 nur anwendbar, wenn die speichernde Stelle die Voraussetzungen für die Berichtigung, Löschung oder Sperrung bei der Erfüllung ihrer laufenden Aufgaben feststellt.

§ 43
Aufhebung bisherigen Rechts

Das Hessische Datenschutzgesetz vom 31. Januar 1978 (GVBl. I S. 96)[2], geändert durch Gesetz vom 14. Oktober 1980 (GVBl. I S. 377), sowie die Hessische Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten vom 1. November 1978 (GVBl. I S. 553)[3] und die Hessische Verordnung über die vom Hessischen Datenschutzbeauftragten zu führenden Dateienregister vom 8. Dezember 1978 (GVBl. I S. 682)[4] werden aufgehoben.

§ 44[5]
Inkrafttreten

Dieses Gesetz tritt am 1. Januar 1987 in Kraft.

[2] Hebt auf GVBl. II 300-19
[3] Hebt auf GVBl. II 300-21
[4] Hebt auf GVBl. II 300-22

[5] § 44 betrifft das Inkrafttreten des Gesetzes vom 11. November 1986. Das Dritte Gesetz zur Änderung des Hessischen Datenschutzgesetzes ist – mit Ausnahme des § 6 – am Tage nach seiner Verkündung in Kraft getreten. § 6 tritt am 1. Juni 1999 in Kraft.
Vorstehend sind die Änderungen des Artikels 1 des Dritten Gesetzes zur Änderung des Hessischen Datenschutzgesetzes eingearbeitet. Die Änderungen anderer Gesetze (Hessisches Krankenhausgesetz, Hessisches Schulgesetz, Hessisches Privatrundfunkgesetz, Gesetz über das Landesamt für Verfassungsschutz) durch Artikel 3 des Gesetzes sind hier nicht enthalten.

3. Bundesdatenschutzgesetz (BDSG)

in der Fassung vom 14. Januar 2003 (BGBl. I S. 66);
zuletzt geändert durch Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I S. 2814)

Abgedruckt ist die am 1. September 2009 gültige Fassung sowie

- gekennzeichnet mit * die alte Fassung des § 28, die gemäß der Übergangsvorschrift § 47 noch partiell bis 31. August 2010 bzw. 31. August 2012 Gültigkeit behält,
- gekennzeichnet mit ** die Vorschriften, die am 1. April 2010 in Kraft treten (Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 [BGBl. I S. 2814] und Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009 [BGBl. I S. 2254]) sowie
- gekennzeichnet mit *** die Vorschriften, die am 11. Juni 2010 in Kraft treten (Artikel 5 des Gesetzes vom 29. Juli 2009 [BGBl. I S. 2355, 2384]).

Inhaltsübersicht

ERSTER ABSCHNITT
Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

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

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Inland in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgegebene oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer
2. zu ihrer Berufsbildung Beschäftigte
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten.

Werden personenbezogene Daten beim Betroffenen 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. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

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

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, dessen Erfüllung die Daten übermittelt werden.

§ 4c Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch

wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
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 offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde eine Übermittlung oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als in § 4b Abs. 1 genannte Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens neun Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zwecke der Übermittlung oder
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

**§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zwecke der Übermittlung oder
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f Beauftragter für den Datenschutz

(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens zwanzig Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für nicht-öffentliche Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der

verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nicht-öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der

Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nicht-öffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nicht-öffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser

Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

**§ 6 Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(3) Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

§ 6a Automatisierte Einzelentscheidung

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

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht des Betroffenen auf Auskunft nach §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

**§ 6a Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) Das Recht des Betroffenen auf Auskunft nach §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten 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 oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht

entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz 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 zweihundertfünfzigtausend Deutsche Mark begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9a Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das

Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1, Abs. 3 und 4 sowie § 44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

ZWEITER ABSCHNITT
Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 13 Datenerhebung

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

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,

3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. 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,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

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

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der

Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

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

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17 (weggefallen)

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 22 Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

> „Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entlässt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in Bezug auf sein Amt erhält. Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministeriums des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, 111 Abs. 5 in Verbindung mit 105 Abs. 1 sowie 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als

ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.

(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und
2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

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

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

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

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte 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 auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 3 und 4 gilt entsprechend.

**§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 4 und 5 gilt entsprechend.

DRITTER ABSCHNITT
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige

Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig:

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,
2. soweit es erforderlich ist
   a) zur Wahrung berechtigter Interessen eines Dritten oder
   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder
3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interessen an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,
2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder
3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung

übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den

Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder Absatz 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene

Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4 a Abs. 3 zulässig. Absatz 2 Nr. 2 Buchstabe b gilt entsprechend.

*§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
   Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse.
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.

(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- oder Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf
   a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   b) Berufs-, Branchen- oder Geschäftsbezeichnung,
   c) Namen,
   d) Titel,
   e) akademische Grade,
   f) Anschrift,

g) Geburtsjahr beschränken und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

In den Fällen des Satzes 1 Nr. 3 ist anzunehmen, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

1. auf strafbare Handlungen,
2. auf Ordnungswidrigkeiten sowie
3. bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten nach Absatz 3 übermittelt werden, der Verarbeitung oder Nutzung zum Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder Absatz 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

**§ 28a Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,
3. der Betroffene die Forderung ausdrücklich anerkannt hat,
4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
   c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und
   d) der Betroffene die Forderung nicht bestritten hat oder
5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

§ 28b Scoring

Zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
2. im Falle der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29, und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
4. im Falle der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

§ 28 Abs. 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der

Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrundeliegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gelten entsprechend.

**§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Abs. 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das

Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrundeliegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gelten entsprechend.

***§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zwecke der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Abs. 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das

Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrundeliegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gelten entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige

Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gelten entsprechend.

§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- und Meinungsforschung

(1) Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt. Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) § 29 gilt nicht.

(5) § 28 Absatz 4 und 6 bis 9 gilt entsprechend.

§ 31 Besondere Zweckbindung

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

§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,
4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
7. die Daten für eigene Zwecke gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder
   b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
8. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,
9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

**§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und
3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder
2. einen Bestandteil des Wahrscheinlichkeitswerts

berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Falle des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die

Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,
2. die verantwortliche Stelle nicht speichert, aber zum Zwecke der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,
2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,
3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie
4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder
2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. Er ist hierauf hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

**§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist. Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt
Aufsichtsbehörde

§§ 36 und 37 (weggefallen)

§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen

anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnitts unterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

VIERTER ABSCHNITT
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

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

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42 Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Die

Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organs der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. §§ 4f und 4g bleiben unberührt.

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nicht-öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
4. personenbezogene Daten zur Bank- und Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der

Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

FÜNFTER ABSCHNITT
Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahren bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einen anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

**§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahren bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einen anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

***§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahren bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einen anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder die Aufsichtsbehörde.

SECHSTER ABSCHNITT
Übergangsvorschriften

§ 45 Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/45/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46 Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

§ 47 Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,
2. für Zwecke der Werbung bis zum 31. August 2012.

§ 48 Bericht der Bundesregierung

Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,
2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29.

Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

5. Grundgesetz für die Bundesrepublik Deutschland (GG) – Auszug

vom 23. Mai 1949 (BGBl. I S. 1);
zuletzt geändert durch Gesetz vom 19. März 2009 (BGBl. I S. 606)
mit Wirkung vom 26. März 2009 bzw. 1. Juli 2009

Artikel 1
Die Würde des Menschen

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2
Freiheit der Person, Recht auf Leben und körperliche Unversehrtheit

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.