UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Saarbrücken, 2012

Merkblatt zur Information über die wichtigsten Bestimmungen des Saarländischen Datenschutzgesetzes und zur Beachtung datenschutzrechtlicher Anforderungen

*Mit dem **Saarländischen Gesetz zum Schutz personenbezogener Daten (Saarländisches Datenschutzgesetz – SDSG)** sind Bereiche des Schutzes personenbezogener Daten, eine Information der damit in Berührung kommenden Personen und die zur Einhaltung des Datenschutzes zu treffenden technischen, personellen und organisatorischen Maßnahmen einschließlich der Kontrollmöglichkeiten grundsätzlich geregelt. Der vollständige Gesetzestext ist im Internet-Angebot des Unabhängigen Datenschutzzentrum Saarland unter http://www.datenschutz.saarland.de im Abschnitt „Datenschutzrecht" enthalten; eine Kenntnisnahme des vollständigen Gesetzestextes wird dringend empfohlen.*

In manchen Verwaltungsbereichen gelten besondere, bereichsspezifische Datenschutzbestimmungen, die den Regelungen des SDSG vorgehen (z. B. im Geschäftsbereich des Ministerium für Soziales, Gesundheit, Frauen und Familie das Sozialgesetzbuch und das Saarländische Krankenhausgesetz, ansonsten im Bereich des Ministerium für Inneres und Sport das Meldegesetz und das Polizeigesetz, im Bereich des Ministerium für Bildung und Kultur die Datenschutzbestimmungen für den Schulbereich).

Zu einer ersten Information und zur leichteren Umsetzung der relevanten Regelungen sollen im Folgenden eine Auswahl der Grundsätze, Grundbegriffe und Regelungen vorgestellt und eventuelle Maßnahmen vorgeschlagen werden, sofern sie nicht schon durch eine entsprechende Dienstanweisung geregelt sind:

Zielsetzung des SDSG (§ 1)

Aufgabe des SDSG ist es, den einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Das Gesetz trägt damit dem vom Bundesverfassungsgericht 1983 im so genannten "Volkszählungsurteil" herausgestellten "Recht auf informationelle Selbstbestimmung" Rechnung, welches Artikel 2 der Saarländischen Landesverfassung als Grundrecht besonders heraushebt.

Der Begriff "Personenbezogene Daten" (§ 3)

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren, natürlichen Person. Auch Daten ohne direkten Personenbezug (z.B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen Bezug genommen werden kann (z.B. Personalnummer, maschinenbezogene Nutzungszeiten bei nur einem in Frage kommenden Benutzer).

Der Begriff "Datenverarbeitung" (§ 3)

Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten, wobei Nutzen jede sonstige Verwendung von Daten ist. Damit unterliegt jede Verwendung personenbezogener Daten dem Datenschutz. Die - inzwischen zum Regelfall gewordene - automatisierte Datenverarbeitung wird wegen ihres Gefährdungspotentials besonders erwähnt und teilweise strengeren Regeln unterworfen. Vgl. hierzu § 10 SDSG.

Zulässigkeit der Datenverarbeitung, Datenvermeidung und Datensparsamkeit (§ 4)

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn das Saarländische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene - in Kenntnis der Bedeutung - eingewilligt hat. Einschränkungen gelten für „sensible“ Daten und für Bewertung von Persönlichkeitsmerkmalen allein durch automatisierte Verfahren. Die Art der Verarbeitung und die dabei genutzte Technik sind so auszurichten, dass so wenige wie möglich personenbezogene Daten verarbeitet werden.

Erforderlichkeit (§§ 12 - 13)

Jede einzelne Phase der Datenverarbeitung ist nur in dem Umfang und solange zulässig, wie ohne sie die Aufgaben der öffentlichen Stelle im konkreten Einzelfall nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden könnten. Bei der Verarbeitung ist die Art und Weise zu wählen, die den Betroffenen am wenigsten beeinträchtigt.

Zweckbindung (§ 13)

Personenbezogene Daten dürfen grundsätzlich nur für die Zwecke (weiter) verarbeitet werden, für die sie erhoben bzw. erstmals gespeichert worden sind; nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine anderweitige Verarbeitung zulässig.

Verpflichtung zur Wahrung des Datengeheimnisses (§ 6)

Allen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten; dies gilt auch nach Beendigung ihrer Tätigkeit. Diese Personen sind über die zu beachtenden Vorschriften über den Datenschutz zu unterrichten (damit ist die frühere Verpflichtung auf den Datenschutz hinfällig).

Sicherstellung des Datenschutzes, behördlicher Datenschutzbeauftragter (§ 7, 8)

Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben für ihren Geschäftsbereich den Datenschutz sicherzustellen. Behördliche Datenschutzbeauftragte unterstützen die verantwortliche Stelle bei der Ausführung der datenschutzrechtlichen Vorschriften und wirken auf deren Einhaltung hin.

Automatisierte Verfahren zur Verarbeitung personenbezogener Daten sind vor ihrem erstmaligen Einsatz und bei wesentlichen Änderungen schriftlich freizugeben. Vor der Freigabe von Verfahren und der Inkraftsetzung von Verwaltungsvorschriften ist die Landesbeauftragte oder der Landesbeauftragte für Datenschutz und Informationsfreiheit zu hören.

Vorabkontrolle (§ 11 Abs. 1)

Vor dem erstmaligen Einsatz von automatisierten Verfahren ist im Rahmen einer Vorabkontrolle zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht entstehen können und welche Maßnahmen dagegen zu treffen sind. Als Grundlage dienen die BSI-Standards zur IT-Sicherheit in Verbindung mit den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik.

Technische und organisatorische Maßnahmen (§ 11 Abs. 2)

Es sind technische und organisatorische Vorkehrungen zu treffen, die den Datenschutz bei der automatisierten Verarbeitung sicherstellen. Hierzu gehören Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Verfügbarkeitskontrolle, gegebenenfalls Auftragskontrolle und zur getrennten Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Das Saarländische Datenschutzgesetz schreibt aufgrund des permanenten technischen Wandels keine konkreten Maßnahmen vor, sondern beschreibt in § 11 deren angestrebten Zweck. Die IT-Sicherheitsrichtlinie legt dazu fest, dass mindestens Maßnahmen für den mittleren Schutzbedarf zutreffen sind, die im IT-Grundschutzhandbuch beschrieben sind. Je nach Sensibilität der Daten sind unter Umständen zusätzliche Maßnahmen notwendig. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind. Als notwendig erkannte Maßnahmen sind auch dann zu treffen, wenn sie die Entwicklung und den Einsatz einer IT-Anwendung erschweren. Sofern Datenschutz (im Interesse der Betroffenen) und Datensicherheit (im Interesse des Dienstbetriebes) mit angemessenen Maßnahmen nicht gewährleistet werden können, muss entweder ein höherer Aufwand in Kauf genommen oder auf den Einsatz der Informationstechnik bzw. des Verfahrens verzichtet werden.

Als regelmäßige Mindestanforderungen sind in einer Dienstanweisung festzulegen:

- Es dürfen nur die Daten verarbeitet werden, die für die Aufgabenerfüllung erforderlich sind. Die bei zulässiger Verarbeitung geltenden Bestimmungen sind einzuhalten.

- Unbefugten Personen ist der Zugang zur Kommunikations- und Informationstechnik und der Zugriff auf Programme und Daten durch geeignete Sicherungsmaßnahmen (z. B. Benutzerkennung und Passwort, Menüsystem, abgestufte Zugriffsberechtigungen) zu verwehren.

- Es darf nur die vor- und freigegebene Hard- und Software eingesetzt werden. Damit ist grundsätzlich der Einsatz privater Hard- und Software und die Benutzung von unlizenzierter, selbst erstellter oder sonst wie beschaffter Software verboten.

- Vorhandene Programme und Daten dürfen nur zur Erfüllung der vorgegebenen Aufgaben genutzt werden. Damit ist auch die Verarbeitung privater Daten mit dienstlichen Mitteln unzulässig. Eine Weitergabe an Dritte darf nicht ohne Erlaubnis erfolgen. Eine Verfälschung ist verboten.

- Daten sind beim Transport (per Datenträger) oder bei der Übertragung (per Datenfernübertragung) vor unbefugtem Lesen, Kopieren, Verändern oder Löschen zu schützen (z.B. durch Verschlüsselung).

- Daten und Programme sind regelmäßig zu sichern und die Sicherungsdatenträger vor missbräuchlichem Zugriff zu schützen.

- Nicht mehr benötigte Daten sind so zu löschen, dass eine missbräuchliche Verarbeitung ausgeschlossen ist; falls erforderlich, ist der Datenträger sicher zu vernichten.

- Für Zwecke der Datensicherung oder der Datenschutzkontrolle gespeicherte Daten (z. B. Logdatei) sind gegen sonstige Nutzung zu sperren und dürfen insbesondere nicht zur Verhaltens- und Leistungskontrolle genutzt werden.

- Bei einer Auftragsdatenverarbeitung (durch Externe; dazu zählen auch Installation, Wartung, Softwarepflege, Reparatur, Vernichtung) dürfen die Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Irreguläre Situationen, z. B. unerwartetes Verhalten, Hinweise auf missbräuchliche Benutzung, Anzeichen von Virenbefall, sind den zuständigen Stellen sofort zu melden.

<u>Übermittlungsregeln (§§14, 16, 17)</u>

Außer zur eigenen Aufgabenerfüllung dürfen personenbezogene Daten auch innerhalb der Stelle an andere Bedienstete oder an andere öffentliche Stellen nur weitergegeben werden, wenn diese sie zur Erfüllung ihrer Aufgaben benötigen; die Verantwortung liegt - außer bei gesetzlich bestimmten Fällen automatisierten Abrufs - beim Übermittler. Bei Übermittlung an Stellen außerhalb des öffentlichen Bereichs sind noch strengere Voraussetzungen zu beachten.

Verfahrensbeschreibung (§ 9)

Für automatisierte Verfahren sind u.a. die verantwortliche Stelle, der Zweck, der wesentliche Inhalt, die Ergebnisse der Vorabkontrolle, die Technik mit Hard- und Software und die Angaben zur Art der Verarbeitung sowie zu den Schutzmaßnahmen in einer Verfahrensbeschreibung festzulegen und auf dem neuesten Stand zu halten.

Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit (§§ 26 - 28)

Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit kontrolliert die Einhaltung der Vorschriften über den Datenschutz. Falls erforderlich, informiert er die zuständigen Aufsichtsbehörden über die Beanstandungen und fordert innerhalb einer bestimmten Frist zur Stellungnahme auf. Er kann Empfehlungen zur Verbesserung geben und die zuständigen Stellen beraten.

Die öffentlichen Stellen sind verpflichtet, der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit und seinen Beauftragten Auskunft auf Fragen zu erteilen, sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Ihnen ist jederzeit - auch unangemeldet - ungehinderter Zutritt zu allen Diensträumen zu gewähren.

Rechte des Betroffenen (§§ 19 - 24)

Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber der verantwortlichen Stelle grundsätzlich das Recht auf Auskunft über gespeicherte Daten, Zweck und Rechtsgrundlage der Speicherung sowie Herkunft und Empfänger von Übermittlungen. Unzutreffende Daten sind zu berichtigen, unzulässig gespeicherte oder nicht mehr erforderliche Daten zu löschen. Bei unklarer Richtigkeit oder nicht möglicher bzw. nicht zulässiger Löschung muss die weitere Verarbeitung durch Sperrung ausgeschlossen werden.

Wird der oder dem Betroffenen durch eine nach den Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung ihrer oder seiner personenbezogenen Daten ein Schaden zugefügt, so ist ihr oder ihm die verantwortliche Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet. In schweren Fällen kann die oder der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Die oder der Ersatzpflichtige haftet jeder oder jedem Betroffenen nach den Sätzen 1 und 2 des § 24 für jedes schädigende Ereignis bis zu einem Betrag von 125.000 Euro.

Jedermann hat das Recht, sich unmittelbar an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt zu sein; dies gilt auch für Bedienstete der öffentlichen Stellen.

Straf- und Bußgeldvorschriften (§ 35, § 36)

Wer unbefugt von dem SDSG geschützte personenbezogene Daten die nicht offenkundig sind verarbeitet, handelt ordnungswidrig; dies kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden. Wer für diese unbefugte Verarbeitung ein Entgelt erzielt oder sie unternimmt, um sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft; schon der Versuch ist strafbar.

Dienst- und arbeitsrechtliche Verantwortlichkeit

Die Missachtung von Sorgfaltspflichten beim Umgang mit personenbezogenen Daten stellt regelmäßig zugleich eine Verletzung von Verpflichtungen aus dem Beschäftigungsverhältnis dar, die zu dienst- oder arbeitsrechtlichen Konsequenzen führen kann.

Allgemeine Strafvorschriften des StGB

(§ 202a Ausspähung von Daten)

Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(§ 203 Verletzung von Privatgeheimnissen, § 204 Verwertung fremder Geheimnisse)

Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis bzw. Einzelangaben über persönliche oder sachliche Verhältnisse eines Anderen, offenbart, das ihm als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichtetem anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr (bei Handeln gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht und bei Verwertung fremder Geheimnisse: zwei Jahren) oder mit Geldstrafe bestraft.

(§ 263a Computerbetrug)

Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft. Auch der Versuch ist strafbar.

(§ 269 Fälschung beweiserheblicher Daten)

Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

(§ 303a Datenveränderung)

Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

(§ 303b Computersabotage)

Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 (Datenveränderung) begeht oder
2. ausgespähte Daten im Sinn von § 202a in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

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

Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu 10 Jahren. Der Versuch ist strafbar.

Kontakt:

Unabhängiges Datenschutzzentrum Saarland

Fritz-Dobisch-Str. 12
66111 Saarbrücken

Tel.: (0681) 94781-0
Telefax: (0681) 94781-29

E-Mail: poststelle@datenschutz.saarland.de
URL: www.datenschutz.saarland.de