Kleines Lexikon zum Datenschutz

TÜV NORD GROUP

Fachstelle für Datenschutz

Anonymisieren

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 (§ 3 Abs. 6 BDSG).

Aufbewahrungsfristen

Aufbewahrungsfristen ergeben sich vor allem aus dem Handelsgesetzbuch (HGB). Geschäftsunterlagen und Handels- und Geschäftsbriefe sowie Unterlagen, die für die Besteuerung wichtig sind, haben Aufbewahrungsfristen von sechs bzw. zehn Jahren. Dazu gehören auch als Dateien gespeicherten Dokumente und E-Mails. Enthalten die aufzubewahrenden Dokumente Datenschutz-rechtlich relevante Inhalte, so geht die Aufbewahrungspflicht der grundsätzlichen Pflicht zur sofortigen Löschung nicht mehr benötigter personenbezogener Daten vor.

Auftragsdatenverarbeitung

Von Datenverarbeitung im Auftrag spricht man, wenn sich die verantwortliche Stelle einer Stelle bedient, die für diese im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt (z. B. Datenerfassungsbüros oder Direktmarketing, Lohn- oder Gehaltsabrechnungen). Lässt ein Unternehmen personenbezogene Daten durch ein Dienstleistungsunternehmen bearbeiten, bleibt die datenschutzrechtliche Verantwortung bei dem beauftragenden Unternehmen. Bei der Auswahl des Auftragnehmers sollte deshalb stets besonderes Augenmerk auf den dortigen Sicherheitsstandard gelegt werden. Die Auftragsvergabe muss schriftlich erfolgen und die Festlegung der Datenverarbeitung (Erhebung, Verarbeitung oder Nutzung), der technischen und organisatorischen Maßnahmen und etwaiger Auftragsverhältnisse umfassen. Dies gilt auch bei Konzerngesellschaften und für die Wartung automatisierter Verfahren und DV-Anlagen (Rechenzentrumsdienstleistungen).

Auskunftsrecht des Betroffenen

Der von der Erhebung personenbezogener Daten Betroffene kann regelmäßig Auskunft verlangen über:

- alle zu seiner Person gespeicherten Daten einschließlich deren Herkunft.
- den Zweck der Speicherung.
- die Empfänger oder die Kategorien der Empfänger, an welche Daten weitergeleitet wurden.
- den Zweck der Weiterleitung.

Die Auskunft muss schriftlich und in der Regel unentgeltlich erteilt werden.

Automatisierte Einzelentscheidung

Automatisiert getroffene Entscheidungen, die für den Betroffenen rechtliche Folgen haben oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich aufgrund einer automatisierten Datenverarbeitung von personenbezogenen Daten getroffen werden, die zur Bewertung von Persönlichkeitsmerkmalen dient (z. B. berufliche Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit, Verhalten). Solche Entscheidungen sind nur zulässig, wenn sie im Rahmen des Abschlusses oder der Erfüllung eines Rechtsverhältnisses ergehen und dem Begehren des Betroffenen stattgegeben wird, oder wenn die Wahrung berechtigter Interessen des Betroffenen durch geeignete technische Maßnahmen gewährleistet sind und der Betroffene hierüber informiert wurde, § 6a BDSG.

Automatisierte Verarbeitung

Eine automatisierte Verarbeitung liegt immer dann vor, wenn personenbezogene Daten unter Einsatz von DV-Anlagen erhoben, verarbeitet oder genutzt werden. (Beispiele: Personal-Datenbank, Bewerber-Daten, Adress-Daten, Lieferanten-Daten)

Betriebsrat

Der betriebliche Datenschutzbeauftragte ist unabhängig in der Ausübung seiner Tätigkeit, deshalb unterliegt er nicht der Kontrolle durch den Betriebsrat. Der Betriebsrat hat allerdings die Aufgabe, die Umsetzung der datenschutzrechtlichen Vorgaben im Unternehmen zu überprüfen. (§ 87 Betr.VG)

Betriebsvereinbarungen

Nach ständiger Rechtsprechung der Arbeitsgerichte sind Betriebsvereinbarungen den Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG gleichzusetzen. Sie können damit Grundlage der Zulässigkeit einer Verarbeitung personenbezogener Daten sein.

Betroffener

Betroffener ist eine natürliche Person, deren personenbezogenen Daten durch die verantwortliche Stelle erhoben, verarbeitet oder genutzt werden.

Bilder

Bilder unterliegen bei ihrer Veröffentlichung, sowohl im Internet als auch in sonstigen Medien, dem Urheberschutz. Grundsätzlich ist die Einwilligung des Berechtigten vor deren Veröffentlichung einzuholen. Auch die Veröffentlichung von Personalfotos in Druckschriften oder im Internet bedarf der Einwilligung sämtlicher abgebildeten Mitarbeiter. Diese kann jederzeit wieder zurückgenommen werden.

Cookies

Cookies sind Informationen, die von einem entsprechend programmierten Web-Server bei dessen Besuch in eine (von der Browser-Software definierte) Datei auf die Festplatte des Besuchers geschrieben und auch wieder ausgelesen werden können. So erhält der Web-Server Informationen über das Navigationsverhalten und damit Informationen über die Interessen des Internetnutzers.

Data Warehouse

Unter Data Warehouse versteht man eine Konzeption zur zentralisierten Datenhaltung und integrierten betriebswirtschaftlichen Auswertung. Die Nutzung erfolgt durch Zusammenführung verschiedener Datensätze.

Umfangreiche Datenbestände werden mit dem Ziel analysiert, Führungsinformationen zur Verfügung zu stellen (z. B. Auskunft über profitable Kunden zu geben, einen verbesserten Kundendienst zu ermöglichen, ein Frühwarnsystem für Geschäftsprozesse zu etablieren oder Produkteinführungen optimal vorzubereiten).

Daten juristischer Personen

Daten juristischer Personen unterliegen grundsätzlich nicht dem Schutz des BDSG. Eine Weitergabe kann ungeachtet dessen jedoch gegen Vorschriften zur Bekämpfung des unlauteren Wettbewerbes, insbesondere des UWG, verstoßen. Datenschutzrechtliche Relevanz kann die Weitergabe von Daten juristischer Personen dann erlangen, wenn Unternehmensdaten in eine Beziehung zu natürlichen Personen (Gesellschaftern, Geschäftsführern oder sonstigen) gebracht werden können.

Datenerhebung

Datenerhebung ist das Beschaffen von Daten über den Betroffenen bei ihm selbst, bei Dritten oder aus sonstigen Quellen.

Datengeheimnis

Alle mit der Datenverarbeitung beschäftigten Personen unterliegen dem Datengeheimnis,

§ 5 BDSG. Es ist Ihnen generell untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Das sog. Datengeheimnis verpflichtet sie, Daten Unbefugten nicht bekannt zu geben oder zugänglich zu machen. Verstöße gegen das Datengeheimnis können neben personellen Konsequenzen auch die Verfolgung als Ordnungswidrigkeit oder gar als Straftat zur Folge haben!

Datennutzung

Datennutzung ist jede sonstige Verwendung von Daten außer Verarbeitung (z. B: Verwendung bereits bedruckter Adressaufkleber).

Datenschutzaufsichtsbehörden - Aufgaben und Befugnisse

Dem jeweiligen Landesdatenschutzbeauftragten stehen als Aufsichts-behörde nachstehende Kompetenzen zu:

- anlassunabhängige Kontrolle
- Einsichtsrecht in Unterlagen und Betreten der Geschäftsräume
- Anordnung nach § 38 Abs. 5 BDSG zur Beseitigung von technischen oder organisatorischen Mängeln (§ 9 BDSG)
- bei Nichtbeseitigung dieser Mängel die Untersagung von Verfahren
- Verlangen der Abberufung betrieblicher Datenschutzbeauftragter, bei nicht hinreichender Fachkunde oder Zuverlässigkeit

Datenschutzbeauftragter

Die Pflicht zur Bestellung von Datenschutzbeauftragten gilt sowohl für Stellen der öffentlichen Verwaltung als auch für privatwirtschaftliche Unternehmungen. Datenschutz-beauftragte müssen bestellt werden, wenn mehr als vier Arbeitnehmer mit der automatisierten oder mindestens zwanzig Mitarbeiter mit der nicht automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind oder die Verarbeitung der Vorabkontrolle unterliegt.

Der Datenschutzbeauftragte muss über fachliche Kenntnisse verfügen und zuverlässig sein. Es darf kein Interessenkonflikt aufgrund der sonstigen von ihm für das Unternehmen ausgeübten Tätigkeit entstehen.

Es können interne oder externe Datenschutzbeauftragte bestellt werden. Entweder kann ein Mitarbeiter des Unternehmens (zusätzlich) mit der Aufgabe des Datenschutzbeauftragten betraut werden oder aber eine natürliche Person außerhalb der verantwortlichen Stelle.

Die Bestellung bedarf zu ihrer Wirksamkeit der Schriftform.

Der Datenschutzbeauftragte wird von der Geschäftsleitung bestellt und ist ihr unmittelbar unterstellt. Er ist weisungsfrei bei der Ausübung seiner Tätigkeit. Das Unternehmen hat die Pflicht, ihn zu unterstützen (z. B. durch Hilfsmittel wie Räume, Einrichtungen, Geräte und Mittel). Der Datenschutzbeauftragte darf wegen seiner Tätigkeit nicht benachteiligt werden. Er hat das Recht zur Anrufung der Aufsichtsbehörde. Betroffene können sich jederzeit an ihn wenden.

Datenübermittlung

Die Bekanntgabe personenbezogener Daten durch die verantwortliche Stelle an einen Dritten wird als Datenübermittlung bezeichnet. Eine Übermittlung von Daten erfolgt dann, wenn die verarbeitende Stelle personenbezogene Daten durch Weitergabe, Einsichtnahme oder Abruf Dritten zukommen lässt. Die Übermittlung oder Nutzung personenbezogener Daten ist zulässig zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen, zur Abwehr von Gefahren für die öffentliche Sicherheit/Verfolgung von Straftaten, bei Gruppendaten in Listenform für Zwecke der Werbung und der Markt- und Meinungsforschung unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen, zur wissenschaftlichen Forschung. Der Betroffene kann der Nutzung oder Übermittlung für Zwecke der Werbung, Markt- oder Meinungsforschung widersprechen. Die Übermittlung sensitiver Daten unterliegt weiteren Voraussetzungen.

Datenübermittlung durch automatisierte Abrufverfahre

Das Verfahren muss angemessen sein, d. h. die schutzwürdigen Interessen der Betroffenen und die Aufgaben oder Geschäftszwecke der beteiligten Stellen müssen berücksichtigt werden. Für das Abrufverfahren sind schriftliche Regelungen zu treffen über Anlass und Zweck, Angaben zum Dritten, an den übermittelt wird und zur Art der zu übermittelnden Daten. Maßnahmen zur Datensicherheit (§ 9) sind zu treffen. Die Abrufe (zumindest Stichproben) und die Zulässigkeit (z. B. Abruf von Schufa-Auskünften) müssen dokumentiert werden.

Datenübermittlung ins Ausland

Für die Übermittlung von personenbezogenen Daten an Stellen in anderen Mitgliedsstaaten der EU, in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder der Organe und Einrichtungen der EG gelten die allgemeinen Regelungen der Datenübermittlung. Dabei findet das Recht des Staates Anwendung, in welchem das die Daten übertragende Unternehmen ansässig ist.

Werden personenbezogene Daten von Deutschland aus in Länder der EU oder des EWR übertragen, gelten die gleichen Anforderungen wie bei einer Übermittlung solcher Daten innerhalb Deutschlands. Die Datenübermittlung in sonstige Staaten unterliegt strengen Anforderungen.

Sie ist nur zulässig, wenn im Drittland ein angemessenes Daten-schutzniveau gewährleistet ist, durch Entscheidungen der EU-Kommission, beim Safe-Harbor-Verfahren (USA), bei vertraglichen Regelungen oder in festgelegten Sonderfällen (z. B. Einwilligung). Personenbezogene Daten dürfen grundsätzlich dann nicht übermittelt werden, wenn das Datenschutzniveau bei der empfangenden Stelle im Vergleich mit den entsprechenden EU-Regelungen als nicht angemessen gilt.

Datensicherheitsmaßnahmen (acht Gebote des Datenschutzes)

§ 9 BDSG und seine Anlagen fordern eine datenschutzkonforme Organisation des Unternehmens bzw. der Behörde. Dabei sind insbesondere acht technische und organisatorische Datenschutz- und Datensicherungsmaßnahmen zu treffen.

- *Zutrittskontrolle* – ist nur räumlich zu verstehen
- *Zugangskontrolle* – Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.
- *Zugriffskontrolle* – Die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen ist zu verhindern.
- *Weitergabekontrolle* – Hierunter fallen sämtliche Aspekte der Weitergabe personenbezogener Daten: elektronische Übertragung, Datentransport, Übermittlungskontrolle.
- *Eingabekontrolle* – Nachvollziehbarkeit, Dokumentation der Datenverwaltung und Pflege.

- *Auftragskontrolle* – Gewährleistung einer weisungsgemäßen Auftragsdatenverarbeitung.
- *Verfügbarkeitskontrolle* – Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
- *Trennungskontrolle* – Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Datenverarbeitung zum Zwecke der Übermittlung

Das BDSG stellt an die kommerzielle Datenverarbeitung zum Zwecke der Übermittlung durch Auskunfteien, Adresshändler oder Markt- und Meinungsforschungsinstitute besondere Anforderungen. Dabei ist grundsätzlich zwischen der Erhebung der Daten zum Zwecke ihrer Weitergabe und der Weitergabe als solcher zu unterscheiden. Bei der Erhebung der Daten muss bereits geprüft werden, ob beim Betroffenen kein Grund zur Annahme eines schutzwürdigen Interesses am Ausschluss der Erhebung, Speicherung oder Veränderung seiner personenbezogenen Daten besteht. Werden die Daten aus allgemein zugänglichen Quellen entnommen, ist zu prüfen, ob ein schutzwürdiges Interesse des Betroffenen besteht, das jenes an der Erhebung, Speicherung oder Veränderung der Daten überwiegt. In diesen Fällen ist bereits die Erhebung der Daten unzulässig. Ferner muss bereits jetzt der Verwendungszweck der zu erhebenden Daten verbindlich festgelegt werden. Eine Änderung dieses Zweckes ist zu einem späteren Zeitpunkt nicht möglich.

Datenvermeidung und Datensparsamkeit

Für das Betreiben von DV-Systemen gilt, dass nur so viel personenbezogene Daten wie unbedingt nötig erhoben, verarbeitet oder genutzt werden sollten. Soweit möglich, ist von Anonymisierung oder Pseudonymisierung Gebrauch zu machen. Diese Grundsätze sollen bereits bei der Planung der technischen Ausführung eines beabsichtigten Datenverarbeitungsprozesses berücksichtigt werden. Hierdurch soll sichergestellt werden, dass die Verarbeitungsvorgänge bereits technisch so ausgestaltet werden, dass so wenige Daten wie möglich in die Erfassung gelangen.

Direkterhebungsgrundsatz

Personenbezogene Daten sind grundsätzlich unmittelbar beim Betroffenen und mit seiner Kenntnis zu erheben.

Eine Abweichung von diesem Grundsatz ist nur in Ausnahmefällen möglich und zwar wenn eine Rechtsvorschrift dies vorsieht, oder wenn die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand erfordern würde.

Dritter

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, nicht jedoch der Betroffene oder die Stelle, die Daten im Auftrag verwendet.

E-Mail

Im Geschäftsverkehr ist die E-Mail mit der normalen Briefpost vergleichbar. Sie gilt als zugegangen, wenn sie den Account des Empfängers erreicht und mit der Kenntnisnahme nach den gewöhnlichen Umständen gerechnet werden kann, also während der üblichen Geschäfts- bzw. Bürozeiten. Gestattet ein Arbeitgeber seinen Arbeitnehmern die Nutzung des Unternehmens-Accounts für private E-Mails, so gilt er als Anbieter eines Teledienstes mit der Folge, dass er zur Wahrung des Fernmeldegeheimnisses gegenüber den Mitarbeitern verpflichtet ist. Private E-Mails der Mitarbeiter sollten von den geschäftlichen E-Mails strikt getrennt werden, da sie unter das Briefgeheimnisfallen, selbst wenn sie auf Speichermedien des Unternehmens verwahrt werden.

Einwilligung des Betroffenen

Die Erfordernis zur Einwilligung ist in § 4 Abs. 1 BDSG geregelt und in ausgestaltet. Die Einwilligung des Betroffenen in die Erhebung personenbezogener Daten muss vor Beginn der Datenerhebung erfolgen (§ 4 Abs. 1 und § 4a BDSG). Dabei ist der Zweck der Erhebung zu nennen. Sie bedarf i. d. R. der Schriftform. Pauschalisierte Einwilligungen und solche ohne zeitliche und inhaltliche Begrenzung sind nicht zulässig. Für die Erhebung sensitiver Daten (§ 3 Abs. 9 BDSG) muss sich die Einwilligung ausdrücklich auf diese beziehen.

Die Veröffentlichung von Mitarbeiterdaten im Internet ist ohne deren Einwilligung nur zulässig, soweit dies zur Erfüllung arbeitsvertraglicher Pflichten erforderlich ist. Die Bekanntmachung privater Daten oder die Veröffentlichung von Bildern sind stets nur mit Zustimmung des betroffenen Mitarbeiters zulässig. Erteilte Einwilligungen sind jederzeit widerrufbar.

Empfänger

Empfänger ist jede Person oder Stelle, die personenbezogene Daten erhält (auch Organisationseinheiten innerhalb der verantwortlichen Stelle).

Europäische Datenschutzrichtlinie

Die europäische Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates) trat am 24. Oktober 1995 in Kraft. Mit ihr wird u.a. sichergestellt, dass in sämtlichen EU-Mitgliedsstaaten der gleiche Datenschutz-Standard gilt. Alle anderen Länder gelten als Drittstaat. Die Umsetzung in nationales Recht erfolgte in Deutschland mit dem Bundesdatenschutzgesetz (BDSG).

Firewall

Unter einer Firewall versteht man Systeme zur Sicherung der unternehmensinternen DV bei Internetverbindungen. Es gibt zahlreiche Möglichkeiten der Realisierung, so z. B. die Filterung bestimmter TCP/IP-Adressen oder die Zwischenschaltung bestimmter Firewall-Server. Das Sicherheitsniveau von Firewalls variiert je nach Aufwand und kann sowohl beim Zugriff nach außen als auch für den Zugriff von außerhalb angelegt werden. Die Rechner wickeln den Datenverkehr zwischen lokalen (internen) Netzen und anderen Netzwerken, in der Regel dem Internet, ab. Jeder Zugriff eines Anwenders auf Daten des externen Netzes erfolgt über den Firewall-Rechner. Dieser lädt die angeforderten Daten und gibt sie an den anfordernden Rechner weiter. Nur der Firewall-Rechner steht in unmittelbarer Verbindung mit dem externen Netz.

Geschäftsmäßige Datenerhebung/-speicherung

Eine geschäftsmäßige Datenerhebung und -speicherung im Sinn des BDSG liegt dann vor, wenn die Datenerhebung/-speicherung als solche den Hauptzweck darstellt. Ziel ist es vor allem, die Daten zu besitzen. Eine geschäftsmäßige Datenerhebung/-speicherung liegt oft dann vor, wenn kein Kontakt mit den Betroffenen besteht, dessen Daten gespeichert werden. In Abgrenzung dazu liegt eine Verwendung zu eigenen Geschäftszwecken dann vor, wenn die Datenerhebung/-speicherung ein Nebenzweck ist, um einen dahinter stehenden eigenen Geschäftszweck zu erreichen (z. B. Abwicklung von eingegangenen Verträgen, Betreuung von Kunden).

Für die Geschäftsmäßigkeit muss außerdem hinzukommen, dass eine Wiederholungs-absicht der Tätigkeit besteht. Ob sie aber gegen Entgelt oder unentgeltlich ausgeübt wird, spielt keine Rolle. Bei einer geschäftsmäßigen Datenerhebung und -speicherung ist auf die Rechtsgrundlagen der § 29, § 30 oder § 30a BDSG zurückzugreifen.

Haftung des externen Datenschutzbeauftragten

Der externe Datenschutzbeauftragte haftet, sofern nichts anderes vereinbart wurde, für Vorsatz und jede Form der Fahrlässigkeit. Die Haftung kann vertraglich eingeschränkt werden. Ein Haftungsausschluss für Vorsatz und grobe Fahrlässigkeit ist jedoch nicht möglich. In jedem Falle kommt lediglich eine Haftung gegenüber dem beauftragenden Unternehmen in Betracht. Eine unmittelbare Haftung gegenüber den Betroffenen besteht nicht.

Haftung des internen Datenschutzbeauftragten

Der interne Datenschutzbeauftragte haftet lediglich im Rahmen der üblichen Arbeitnehmerhaftung gegenüber dem Unternehmen. Eine unmittelbare Haftung gegenüber den Betroffenen besteht nicht.

Heimarbeitsplätze

Werden Mitarbeiter an Heimarbeitsplätzen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt, so ist dafür Sorge zu tragen, dass auch hier das gesetzliche vorgeschriebene Datenschutzniveau gewährleistet wird.

Informationelles Selbstbestimmungsrecht

Das Recht auf informationelle Selbstbestimmung ist im bundesdeutschen Recht das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es handelt sich dabei nach der Rechtsprechung des Bundesverfassungsgerichts um ein Datenschutz-Grundrecht, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird. Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit.

Das Recht auf informationelle Selbstbestimmung leitet sich nach Ansicht des Europäischen Parlamentes auch aus Artikel 8 Absatz 1 der Europäischen Menschenrechtskonvention ab:

„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.“ (EMRK Art. 8 Abs. 1)

Das Recht auf informationelle Selbstbestimmung ist weit gefasst. Es wird nicht unterschieden, ob mehr oder weniger sensible Daten des Einzelnen betroffen sind. Das Bundesverfassungsgericht stellte fest, dass unter den Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen könne und es insoweit keine belanglosen Daten gebe.

Einschränkungen des Grundrechts seien zwar möglich, bedürften aber einer gesetzlichen Grundlage. Dabei habe der Gesetzgeber abzuwägen zwischen dem Geheimhaltungsinteresse des Betroffenen und dem öffentlichen Informationsinteresse der verarbeitenden Stelle. Einschränkungen sind nur zulässig im überwiegenden Allgemeininteresse. Sie bedürfen einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muss. Es wird differenziert zwischen

Maßnahmen, die ohne oder gegen den Willen des Betroffenen vorgenommen werden, und solchen, die freiwillig erfolgen.

Für erstere muss die gesetzliche Ermächtigung auch „bereichsspezifisch, präzise und amtshilfefest“ sein. (Volkszählungsurteil, BVerfGE 65, 1, 46).

Zudem kann man unterscheiden zwischen anonymisierten Daten, die keinen Rückschluss auf den Betroffenen zulassen (z. B. für statistische Erhebungen), und zwischen Daten, die personalisierbar sind. Bei anonymisierten Daten ist die Zweckbindung gelockert, für Daten, die personalisierbar sind, gilt eine strenge Zweckbindung. Der Gesetzgeber muss Vorkehrungen treffen, um Datenmissbrauch zu verhindern (Verfahrensvorschriften, Datenschutzbeauftragte,...). Das informationelle Selbstbestimmungsrecht wurde die Grundlage für die bestehenden Datenschutzgesetze wie das Bundesdatenschutzgesetz oder die Landes-datenschutzgesetze und beeinflusste auch die Entwicklung der Richtlinie 95/46/EG (Datenschutzrichtlinie). Auch in jüngerer Zeit hat das Recht auf informationelle Selbstbestimmung in der verfassungs-gerichtlichen Rechtsprechung eine große Rolle gespielt. So wurde die Rasterfahndung in Nordrhein-Westfalen für verfassungswidrig erklärt; die §§ 100c und 100d StPO (der sogenannte Große Lauschangriff) mussten um einen Straftatenkatalog und um explizite Löschungsvorschriften ergänzt werden (BVerfGE 109, 279).

Kontrolle des Datenschutzes

Im Bereich der privaten Wirtschaft sind zunächst die Unternehmen als speichernde Stellen selbst für sie Einhaltung der Datenschutzstandards verantwortlich. Daneben bestehen Überwachungs- und Kontrollkompetenzen des jeweiligen Landesdatenschutzbeauftragten als Aufsichtsbehörde. Bei Fragen oder in Zweifelsfällen können sich die betrieblichen Datenschutzbeauftragten an die Aufsichtsbehörde wenden. Die Aufsichtsbehörde ist auch zuständig für die Vorabkontrolle bei meldepflichtigen Vorgängen.

Konzerndatenschutz – Datenschutz im Unternehmensverbund

Jedes einzelne Unternehmen eines Konzerns (Zusammenschluss mehrerer selbständiger juristischer Personen unter einer einheitlichen Führung), ist zur Bestellung eines Datenschutzbeauftragten verpflichtet, sofern die Anforderungen des § 4f BDSG erfüllt sind. Es kann ein Konzerndatenschutzbeauftragter bestellt werden. Dieser ist in der Firma, welche ihn als Arbeitnehmer beschäftigt, interner und in den anderen Unternehmen des Konzerns externer Datenschutzbeauftragter.

Konzernprivileg

Ein Konzernprivileg, wie es in anderen Rechtsgebieten vorhanden ist, kennt das BDSG nicht. Die Übermittlung personenbezogener Daten zwischen einzelnen juristischen Personen innerhalb eines Konzern unterfällt somit uneingeschränkt den Regelungen des BDSG.

Kundenbindungssysteme

Kundenbindungssysteme wie z. B. Payback- oder sonstige Bonuskarten werden in den meisten Fällen den datenschutzrechtlichen Anforderungen nicht gerecht. Häufigste Gründe für Beanstandungen sind unzureichende Einwilligungen der Kunden, die Erhebung nicht erforderlicher Daten, die Weiterleitung an andere Stellen, wenn sich mehrere Unternehmen für die Herausgabe von Payback-Karten zusammengeschlossen haben oder das Erstellen detaillierter Kundenprofile.

Löschung vorhandener personenbezogener Daten

Unter Löschung personenbezogener Daten versteht man deren unwiederbringliche Vernichtung. Personenbezogene Daten sind unverzüglich zu löschen beim Wegfall des Grundes ihrer Erhebung, bei unzulässigen Daten und bei besonderen Datenarten oder Daten über Strafhandlungen oder Ordnungswidrigkeiten, deren Richtigkeit nicht bewiesen ist. Es ist nicht zulässig, Daten zur späteren Verwendung “auf Vorrat” zu speichern.

Meldepflicht

Die verantwortliche Stelle hat Verfahren automatisierter Verarbeitung vor der Inbetriebnahme der Aufsichtsbehörde zu melden. Keine Meldepflicht besteht, wenn ein Datenschutzbeauftragter bestellt ist. Für Adresshändler, Auskunfteien, Markt- und Meinungsforschungsinstitute gilt diese Ausnahmeregelung nicht.

Mobile personenbezogene Speicher- und Verarbeitungsmedien (Chipkarten)

Dies sind an den Betroffenen ausgegebene Datenträger, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende Stelle automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann. Der Betroffene ist über: den Herausgeber und seine Anschrift, die Funktionsweise und Art der zu verarbeitenden Daten, die Wahrung seiner Rechte und die zu treffenden Maßnahmen bei Verlust oder Zerstörung zu unterrichten. Geräte zur Auskunftserteilung sind unentgeltlich zur Verfügung zu stellen. Beispiele: Geldkarten der Banken, Chipkarten zu modernen Zeiterfassungssystemen.

Newsletter

Der Versand von Newslettern per E-Mail ist, auch wenn diese Werbung beinhalten, zulässig, soweit der Empfänger dem zuvor zugestimmt hat. Die Anfrage, ob zukünftig Newsletter übersandt werden dürfen, stellt jedoch eine unzulässige E-Mail-Werbung dar.

Nicht-öffentliche Stelle

Nicht-öffentliche Stellen im Sinn des Datenschutzes sind definiert in § 2 Absatz 4 des BDSG. Darunter fallen Stellen in privat-rechtlicher Organisation (also GmbH, AG, KG, OHG, Vereine usw.) sowie natürliche Personen (z.B. Einzelfirma, Selbstständige und Freie Berufe), nicht aber Privatpersonen.

Nicht-automatisierte Dateien

Nicht-automatisierte Dateien sind nicht-automatisierte Sammlungen von personenbezogenen Daten, die gleichartig aufgebaut sind und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können.

Personalaktenführung

Der Arbeitgeber muss stets bei der Personalaktenführung folgende Grundsätze berücksichtigen:

- Grundsatz der Transparenz gegenüber dem betroffenen Mitarbeiter
- Grundsatz der Aktenwahrheit; die Inhalte der Akten müssen zutreffend sein
- Grundsatz der Zulässigkeit; die Erhebung der in den Personalakten befindlichen Daten muss zulässig sein
- Grundsatz der Vertraulichkeit von Personalakten

Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), soweit sie nicht ausschließlich für familiäre oder persönliche Zwecke verwendet werden. Daten über persönliche Verhältnisse sind z. B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit Beruf, Konfession, Krankheiten; Angaben über sachliche Verhältnisse sind z. B. Angaben zu Einkommen, Eigentumsverhältnissen, KFZ-Typ, Steuern, Versicherungen. Besondere personenbezogene Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Sie dürfen nur unter bestimmten Voraussetzungen verwendet werden. Diese Daten unterliegen der Vorabkontrolle durch den DSB.

Robinsonliste

Die Robinsonliste wird vom Deutschen Direktmarketingverband geführt und enthält Einträge von Personen, die keine Zusendungen von Werbematerial erhalten wollen. Die Beachtung der Robinsonliste beruht auf Freiwilligkeit.

Safe Harbor

Safe Harbor (englisch für „Sicherer Hafen“) ist eine besondere Datenschutz-Vereinbarung zwischen der Europäischen Union und den Vereinigten Staaten, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln.

Die Richtlinie 95/46/EG (Datenschutzrichtlinie) verbietet es grundsätzlich, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutz-niveau verfügen. Dies trifft auf die USA zu, da diese keine umfassenden gesetzlichen Regelungen kennen, die den Standards der EG entsprechen.

Damit der Datenverkehr zwischen den USA und der EU nicht zum Erliegen kommt, wurde zwischen 1998 und 2000 ein besonderes Verfahren entwickelt. US-Unternehmen können dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles (englisch für „Grundsätze des sicheren Hafens“) und die dazugehörenden – verbindlichen – Frequently Asked Questions (FAQ) zu beachten. Im Jahr 2000 hat die EU anerkannt, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein ausreichender Schutz besteht. Bislang sind mehr als eintausend Unternehmen dem Safe-Harbor-Abkommen beigetreten, darunter Microsoft, General Motors, Amazon, Google, Hewlett-Packard, Facebook u.a..

Schadensersatz

Wird dem Betroffenen durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner Daten ein Schaden zugefügt, ist die verantwortliche Stelle oder der Träger zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Schulung interner Datenschutzbeauftragter

Mitarbeiter, die zum internen Datenschutzbeauftragten bestellt werden sollen, müssen neben ihrer persönlichen Zuverlässigkeit und Kenntnissen innerbetrieblicher Abläufe auch über die zur Erfüllung dieser Aufgabe erforderliche Sachkunde verfügen. Ein Nachweis hierüber kann durch die Teilnahme an entsprechenden Schulungen erbracht werden.

Schulung von Mitarbeitern

Der Datenschutzbeauftragte muss die im Unternehmen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigten Mitarbeiter im Rahmen regelmäßiger Schulungen über neue Entwicklungen der gesetzlichen Bestimmungen zum Datenschutz sowie über die bereits getroffenen oder zu erwartenden innerbetrieblichen Maßnahmen unterrichten.

Sperrdatei

Hat ein Betroffener Widerspruch gegen die Nutzung seiner persönlichen Daten zum Zwecke der Werbung eingelegt, muss sichergestellt werden, dass dieser Widerspruch auch bei späteren Werbeaktionen. Hierzu ist es erforderlich, diesen Adressaten in eine Sperrdatei aufzunehmen.

Sperrung von Daten

Unter Sperrung personenbezogener Daten ist deren Kennzeichnung zu verstehen, ihre weitere Verarbeitung oder Nutzung einzuschränken. In besonderen Fällen besteht die Pflicht, Daten zu sperren.

Wenn personenbezogene Daten eigentlich gelöscht werden müssten, dies aber aufgrund satzungsmäßiger oder gesetzlicher Aufbewahrungsfristen nicht möglich ist, eine Löschung die schutzwürdigen Interessen des Betroffenen beeinträchtigen würde oder die Löschung aufgrund der Art der Datenspeicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich wäre, dann müssen die Daten gesperrt werden. Personenbezogene Daten sind auch dann zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Gesperrte Daten dürfen in der Regel nicht ohne Einwilligung des Betroffenen genutzt oder übermittelt werden.

Straf- und Bußgeldvorschriften

Das BDSG enthält in den §§ 43 und 44 Ordnungswidrigkeits- und Straftatbestände. Als Sanktionen können Bußgelder von bis zu 50.000 Euro Geldstrafen und Freiheitsstrafen von bis zu zwei Jahren verhängt werden.

Mit Geldbußen kann belegt werden, wer der Meldepflicht nicht nachkommt, einen Beauftragten für den Datenschutz nicht ordnungsgemäß bestellt, Betroffene nicht ordnungsgemäß über Widerspruchsrechte informiert, Daten inkorrekt übermittelt oder nutzt, Gründe zur Datenübermittlung nicht aufzeichnet, Betroffene nicht ordnungsgemäß benachrichtigt, bestrittene Daten ohne Gegendarstellung übermittelt, Prüfungen der Aufsichtsbehörde behindert oder vollziehbare Anordnungen der Aufsichtsbehörde nicht beachtet.

Mit Geldbußen bis zu 300.000 Euro wird belegt, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet, zum Abruf mittels automatisierten Verfahrens bereithält, abruft oder sich oder einem anderen verschafft, die Übermittlung durch unrichtige Angaben erschleicht, Daten entgegen der Zweckbegrenzung an Dritte weitergibt oder anonymisierte Daten mit Einzelangaben von Betroffenen zusammenführt. Werden solche Handlungen gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern begangen, stellt dies einen Straftatbestand dar. Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafe können die Folge sein. Ebenfalls mit Freiheits- oder Geldstrafe wird das Ausspähen von Daten sanktioniert.

Darüber hinaus können Verstöße gegen Datenschutzgrundsätze die zivilrechtliche Haftung auf Schadensersatz zur Folge haben.

Stapelverarbeitung von Daten

Unter der Stapelverarbeitung ist der Abruf oder die Übermittlung eines Gesamtbestandes an Daten zu verstehen, § 10 Abs. 4 S. 4 BDSG.

Technisch-organisatorische Maßnahmen

Das Bundesdatenschutzgesetz fordert in § 9, dass technische und organisatorische Maßnahmen von der verantwortlichen Stelle zu treffen sind, die erforderlich sind, um die Vorschriften des BDSG umzusetzen. Mit dieser Norm bindet der Gesetzgeber die IT-Sicherheit in das Datenschutzrecht ein. Die technisch-organisatorischen Maßnahmen, die eingehalten werden sollen, werden in der Anlage zu § 9 BDSG abschließend aufgelistet.

Dazu zählen im Einzelnen: Zutritts-, Zugangs-, Zugriffs-, Eingabe-, Weitergabe-, Auftrags- und Verfügbarkeitskontrolle sowie das Trennungsgebot. Ebenfalls wird in § 9 Satz 2 des BDSG präzisiert, dass die Maßnahmen verhältnismäßig sein müssen, also in einem angemessenen Verhältnis zu ihrem jeweils angestrebten Schutzzweck stehen sollten.

Telefaxwerbung

Ohne das vorherige Einverständnis des Beworbenen ist Telefaxwerbung sowohl im privaten, als auch im gewerblichen Bereich unzulässig. Faxwerbung ohne Einwilligung verstößt nicht nur gegen die Grundsätze des Datenschutzes, sondern auch gegen die guten Sitten im Sinne des § 1 UWG. Ist der Empfänger ein Gewerbetreibender, kommt darüber hinaus auch ein unzulässiger Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb in Betracht.

Telefonmarketing

Telefonmarketing ist gegenüber Privatpersonen nur dann zulässig, wenn diese zuvor ihr Einverständnis hierzu abgegeben haben, unabhängig davon, ob Neukunden geworben werden sollen, oder der Anruf der Kundenpflege oder -rückgewinnung dient.

Telemediengesetz / Telekommunikationsgesetz

Das Telekommunikationsgesetz (TKG) regelt unter anderem den Datenschutz in der Telekommunikation (Internet- und E-Mail-Zugang, Telefon u.a.). Zum Zug kommt das TKG insbesondere bei der privaten Nutzung von betrieblichen Telekommunikationsanlagen. Hier gilt der Arbeitgeber als geschäftsmäßiger Anbieter von Telekommunikations-diensten (im Sinn von § 3 Nr. 6 TKG).

Nur falls eine private Nutzung nicht geduldet wird, ist der Arbeitnehmer nicht „Dritter“ und die Nutzung erfolgt nicht zu fremden Zwecken - das TKG ist dann nicht anwendbar.

Das Telemediengesetz (TMG) regelt die rechtlichen Rahmenbedingungen für Telemedien, d.h. im Wesentlichen Internet-Angebote, in Deutschland. Das TMG hat mit seinem Inkrafttreten folgende Normen abgelöst:

- Teledienstegesetz (TDG)
- Teledienste-Datenschutzgesetz (TDDSG)
- Mediendienste-Staatsvertrag (MDStV)

Relevant ist überwiegend Abschnitt 4 TMG. Dieser Abschnitt regelt den Datenschutz zwischen Telemedien-Anbietern und Nutzern.

Tragbarer PC (Laptop/Notebook/Handheld)

Die Speicherung personenbezogener Daten auf mobilen Geräten ist insbesondere problematisch, wenn dieses unverschlüsselt erfolgt. Wird ein mobiles Gerät gestohlen oder an einem privaten, nicht hinreichend gesicherten Anschluss mit dem Internet verbunden, ist der erforderliche Datenschutz nicht mehr gewährleistet. Sensible Daten sollten deshalb nach Möglichkeit nicht auf mobilen Geräten gespeichert werden. Ist dies unumgänglich, sollte die Speicherung stets in verschlüsselter Form erfolgen. Sensible Daten dürfen auf mobilen Geräten nur dann verarbeitet werden, wenn dies aufgrund der Aufgabenerfüllung unvermeidbar ist. Falls sensible bzw. personenbezogene Daten verarbeitet werden müssen, ist die Installation von Sicherheitssoftware zwingend erforderlich.

Übermittlung von Daten

Eine Übermittlung von Daten erfolgt dann, wenn die verarbeitende Stelle personenbezogene Daten durch Weitergabe, Einsichtnahme oder Abruf Dritten zukommen lässt. Eine bloße Bereitstellung dieser Daten zum Abruf genügt hingegen nicht.

Veränderung von Daten

Verändern ist das inhaltliche Umgestalten personenbezogener Daten.

Verantwortliche Stelle

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.

Verarbeitung von Daten

Verarbeiten von personenbezogenen Daten ist deren Speichern, Verändern, Übermitteln, Sperren oder Löschen. Besonders strengen Anforderungen unterliegt die Verarbeitung besonders sensitiver personenbezogener Daten unterliegt.

Eine automatisierte Verarbeitung personenbezogener Daten ist immer dann gegeben, wenn die Erhebung, Verarbeitung oder Nutzung unter dem Einsatz von Datenverarbeitungsanlagen erfolgt, § 3 Abs. 2 BDSG.

Verarbeitung von Daten, nicht automatisierte

Nicht-automatisierte Dateien sind nicht-automatisierte Sammlungen von personenbezogenen Daten, die gleichartig aufgebaut sind und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können. Hierfür genügt bereits eine alphabetische Ordnung, sofern personenbezogene Angaben als Suchkriterien für die Erhebung, Verarbeitung oder Nutzung fungieren.

Verarbeitungsübersicht

Eine Verarbeitungsübersicht listet alle Arten und Methoden auf, über oder mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden z.B. Personalverwaltung oder Kundenbetreuung). Zudem muss aus ihr erkennbar sein, ob die die Verarbeitung datenschutzrechtlich hinreichend gesichert ist. Dazu sind die technisch-organisatorischen Maßnahmen nach § 9 BDSG einschlägig. Die gesetzliche Regelung beruht hierzu auf § 4e Nr. 9 BDSG.

Verfahrensverzeichnis

Jedermann hat das Recht auf Offenlegung des Unternehmens, welche personenbezogenen Daten zu welchem Zweck gespeichert und ggf. weitergegeben werden. Das Unternehmen hat dem Datenschutz-beauftragten Verzeichnisse der meldepflichtigen Verfahren zur Verfügung zu stellen. Diese bilden die Grundlage des betrieblichen Datenschutzes. Ihr Inhalt richtet sich nach § 4e BDSG. Die Verfahrensübersicht muss eine hinreichende Aussagekraft haben und sich stets auf aktuellem Stand befinden. Das Verfahrensverzeichnis besteht aus einem öffentlichen und einem nicht öffentlichen Teil. Der öffentliche Teil muss auf Anfrage jedem Interessenten zugänglich gemacht werden. Grundsätzlich genügt es, wenn dieses im Internet abrufbar ist.

Videoüberwachung

Videoüberwachung ist zulässig zur Beobachtung öffentlich zugänglicher Räume (z. B. Eingangsbereiche, Verkaufsräume, Schalterhallen, Zaun-anlagen) sowie Verarbeitung und Nutzung der Aufnahmen zur

- Aufgabenerfüllung öffentlicher Stellen,
- Wahrnehmung des Hausrechts oder
- Wahrnehmung berechtigter Interessen für konkrete Zwecke.

Die Zwecke der Überwachung müssen vorab konkret festgelegt und dokumentiert werden. Es besteht die Pflicht zur Information. Die betreffenden Bereiche müssen entsprechend gekennzeichnet sein.

Es ist erkennbar zu machen, dass überwacht wird und wer dies tut Unmittelbar, wenn Zweck erreicht ist, müssen der erhobenen Daten gelöscht werden. Nicht betroffen sind die Überwachung von rein privaten Räumen oder Geländen sowie die Überwachung des Arbeitsplatzes. Letztere kann jedoch anderweitigen Bestimmungen unterliegen.

Vorabkontrolle

Der Datenschutzbeauftragte hat eine Vorabkontrolle durchzuführen, wenn es um sensitive Daten geht oder die Persönlichkeit des Betroffenen bewertet werden soll. Automatisierte Verarbeitungen personenbezogener Daten müssen bereits vor ihrem Beginn geprüft werden, sofern sie besondere Risiken für die Rechte und Freiheiten der Betroffenen bergen. Dies ist immer dann der Fall, wenn besonders sensitive Daten im Sinne des § 3 Abs. 9 BDSG zur Verarbeitung gelangen sollen, oder wenn die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten und Leistungen zu bewerten, § 4d Abs. 5 BDSG.

Die Kontrolle ist schriftlich zu dokumentieren und sollte mindestens eine Stellungnahme enthalten. Gegenstand der Prüfung ist die Zulässigkeit des beabsichtigten Verfahrens sowie die Feststellung, ob eine den speziellen Risiken entsprechende Vorsorge getroffen wurde.

Widerspruchsrecht

Personenbezogene Daten dürfen nicht verwendet werden, wenn der Betroffene wegen seiner besonderen persönlichen Situation widerspricht und sein Interesse höher zu bewerten ist als das der verantwortlichen Stelle (sofern keine Verpflichtung durch eine Rechtsvorschrift besteht).

Der Betroffene hat ein zusätzliches Widerspruchsrecht bei Nutzung seiner Daten für Zwecke der Werbung, Markt- oder Meinungsforschung.

Zulässigkeit der Datenverarbeitung im nicht öffentlichen Bereich

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist grundsätzlich nur dann zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Im Bereich der privaten Wirtschaft ist die Verarbeitung personenbezogener Daten für eigene Zwecke grundsätzlich zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses (z. B. Arbeitsvertrag) oder vertragsähnlichen Vertrauensverhältnisses (z. B. Bewerbung), zur Wahrung berechtigter Interessen der verantwortlichen Stelle unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen oder wenn die Daten aus öffentlichen Quellen entnommen werden können.

Strengere Anforderungen sind an die Verarbeitung personenbezogener Daten für fremde Zwecke geknüpft. Diese ist nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Verarbeitung hat.

Zulässigkeit der Datenverarbeitung im öffentlichen Bereich

Im öffentlichen Bereich ist das Verarbeiten personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

Zulässigkeit der Erhebung, Verarbeitung und Nutzung besonderer Arten von personenbezogenen Daten

Die Erhebung, Verarbeitung und Nutzung besonderer Arten personenbezogener Daten ist zulässig:

- bei Einwilligung des Betroffenen.
- ohne Einwilligung, wenn dies aus lebenswichtigem Interesse des Betroffenen oder Dritten erforderlich ist, und er selbst keine Einwilligung geben kann.
- die Daten vom Betroffenen offenkundig öffentlich gemacht wurden.

- dies für rechtliche Ansprüche erforderlich ist und das schutzwürdige Interesse des Betroffenen dagegen nicht überwiegt.
- dies zur wissenschaftlichen Forschung erforderlich ist.
- dies aus Gesundheitszwecken erforderlich ist und das Personal der Geheimhaltungspflicht unterliegt.

Zweckbestimmung

Personenbezogene Daten dürfen nur dann erhoben werden, wenn vorab ihre Zweckbestimmung festgelegt wurde. Zulässig ist die Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses (z. B. Arbeitsvertrag) oder vertragsähnlichen Vertrauensverhältnisses (z. B. Bewerbung), zur

Wahrung berechtigter Interessen der verantwortlichen Stelle unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen oder wenn die Daten aus öffentlichen Quellen entnommen werden können. Über den Zweck muss der Betroffene informiert werden. Eine nur vage Definition der Zweckbestimmung genügt nicht. Sie muss so deutlich wie möglich formuliert werden. Eine vom ursprünglichen Zweck abweichende Bearbeitung oder Nutzung personenbezogener Daten ist ohne die erneute Einwilligung des Betroffenen nicht zulässig.

Stand: Februar 2010

Ansprechpartner

Peter Kattner, LL.M.

IT Security
Fachstelle für Datenschutz

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen

Tel.: +49 201 8999-643
Fax: +49 201 8999-666
p.kattner@tuvit.de
www.tuvit.de

Jörg Schließke, LL.B.

IT Security
Fachstelle für Datenschutz

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen

Tel.: +49 201 8999-533
Fax: +49 201 8999-666
j.schlisske@tuvit.de
www.tuvit.de