Datenschutzordnung

BUND WESTFÄLISCHER KARNEVAL E.V.
Vereinigung zur Förderung heimatlichen
Fastnachtsbrauchtums

Sitz: Münster in Westfalen

ORDNUNGEN

Stand: 25. Oktober 2015

Inhaltsverzeichnis

Datenschutzordnung
Bund Westfälischer Karneval e.V.

Als Ergänzung zu § 19 der Satzung regelt diese Datenschutz-Ordnung die Erhebung, automatisierte Verarbeitung - Speicherung, Übermittlung, Löschung - und Nutzung personenbezogener Daten, die für die Erfüllung des Verbandszwecks erforderlich sind. Sie gilt für den Bund Westfälischer Karneval e.V. (nachfolgend: BWK) und die ihm angeschlossenen Mitgliedsgesellschaften (nachfolgend: Mitglieder).

§ 1 Datenerhebung, -speicherung und -verarbeitung

(1) Die Mitgliedschaft im BWK ist als vertragsähnliches Vertrauensverhältnis anzusehen, dessen Rahmen und Inhalt im Wesentlichen durch die Satzung vorgegeben ist. Aus dem Vertrauensverhältnis folgt, dass der BWK bei der Erhebung, Verarbeitung und Nutzung von Daten das Persönlichkeitsrecht seiner Mitglieder angemessen berücksichtigen muss. Mitgliederdaten dürfen im Rahmen des Verbandszwecks erhoben, verarbeitet oder genutzt werden (§ 28 Abs. 1 Nr. 1 BDSG).

(2) Der BWK erfasst ausschließlich für die Erfüllung seiner satzungsgemäßen Zwecke und Aufgaben personenbezogene und andere Daten von seinen Mitgliedern bzw. von deren Mitgliedern sowie von Funktionsträgern seiner nachgeordneten Strukturen.

(3) Diese Daten werden ggf. in dem verbandseigenen EDV-System der Geschäftsstelle und/oder in den EDV-Systemen der zuständigen Mitglieder des Präsidiums oder der vom Präsidium beauftragten Funktionsträger gespeichert.

(4) Erfasst werden insbesondere folgende Angaben:
Name, Vorname, Anschrift, Kommunikationsdaten, Mitgliedsnummer sowie bei Notwendigkeit auch die Bankverbindung. Bei Funktionsträgern und Teilnehmer/innen an Lehrgängen können zusätzlich Angaben zu Lizenzen und deren Gültigkeit sowie Geburtsdaten erfasst werden.

(5) Sonstige Informationen zu den Mitgliedern, zu deren Mitgliedern und Informationen über Nichtmitglieder werden vom BWK grundsätzlich nur erhoben, verarbeitet oder genutzt, wenn sie zur Aufrechterhaltung oder Förderung des Verbandszwecks notwendig sind (z.B. Kontaktdaten einzelner Mitglieder) und keine Anhaltspunkte bestehen, dass die betroffene Person ein schutzwürdiges Interesse hat, das der Erhebung, Verarbeitung oder Nutzung entgegensteht (§ 28 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1 BDSG).

(6) Besondere personenbezogene Daten werden vom BWK nicht erhoben, verarbeitet oder genutzt (§ 3 Abs. 9 BDSG).

(7) Die Datenerhebung erfolgt nach dem Prinzip der Datensparsamkeit.

§ 2 Datennutzung

(1) Nur Präsidiumsmitglieder und sonstige Personen, die im BWK eine besondere Funktion ausüben, welche die Kenntnis bestimmter Daten erfordert, erhalten die entsprechenden Daten soweit zur Funktionsausübung notwendig.

(2) Die personenbezogenen Daten werden zum Beispiel zu Folgendem verwendet:

- Mitgliederverwaltung
- Abonnentenverwaltung
- Lehrgangsverwaltung
- Sportverwaltung (Trainerausweise, Veröffentlichung von Turnierergebnissen, Meldewesen für Tanzturniere, Lizenzwesen)
- Ehrungsverwaltung (Antragstellung, Urkunden, Veröffentlichung in Verbandsmedien)
- Funktionsträgerverwaltung
- Beratung und Information durch Fachausschüsse

Die vereinsbezogenen Daten werden zum Beispiel für folgendes verwendet:

- Ansprechpartnerverwaltung
- Beitragsverwaltung
- Turnierwesen

(3) Ausscheidende Funktionsträger des Verbandes verpflichten sich, alle Unterlagen und Datenträger an den Nachfolger zu übergeben und die Dateien auf privaten PC's unwiederbringlich zu löschen und dies auch vom Datenschutzbeauftragen überprüfen zu lassen.

§ 3 Datenübermittlung

(1) Als Mitglied der Närrischen Europäischen Gemeinschaft (NEG), des Bundes Deutscher Karneval e.V. (BDK), des Landesverbandes für karnevalistischen Tanzsport Nordrhein-Westfalen e.V. (LkT-NRW), der Karnevalsjugend Nordrhein-Westfalen e.V. (KaJu-NRW) sowie den zu diesen Organisationen zählenden Dachverbänden stellt der BWK ausschließlich die zur Sicherung der satzungsgemäßen Zwecke der Dachorganisationen notwendigen personen- und vereinsbezogenen Daten nach Aufforderung zur Verfügung. Dabei ist die Übermittlung im Einzelfall auf das absolut notwendige Maß beschränkt.

(2) Der BWK hat Versicherungen abgeschlossen oder schließt solche ab, aus denen er, seine Funktionsträger und/oder seine Mitglieder Leistungen beziehen können. Soweit dies zur Begründung, Durchführung oder Beendigung dieser Verträge erforderlich ist, übermittelt der BWK personenbezogene Daten der betreffenden Personen an das zuständige Versicherungsunternehmen. Der BWK stellt hierbei vertraglich sicher, dass der Empfänger die Daten ausschließlich dem Übermittlungszweck entsprechend verwendet.

(3) Der BWK übermittelt seinen Kooperationspartnern (z.B. GEMA, KSK), mit denen eine vertraglich geregelte Zusammenarbeit besteht, Daten von Mitgliedern und ggf. Funktionsträgern, die auf Name und Anschrift beschränkt sind, ausschließlich auf Anforderung und zu vertraglich geregelten Zwecken,

die im Interesse des jeweiligen Mitglieds sind und dem satzungsgemäßen Zweck des BWK entsprechen. Die Kooperationspartner werden darauf hingewiesen, dass die Daten nur für eigene Zwecke verwendet werden dürfen und somit eine weitere Übermittlung (auch zwischen zwei Kooperationspartnern des BWK) unzulässig ist.

§ 4 Weitergabe von Mitgliederdaten an BWK-Mitglieder

(1) Macht ein Mitglied glaubhaft, dass es die Mitgliederliste zur Wahrnehmung seiner satzungsgemäßen Rechte benötigt, wird ihm eine gedruckte Kopie der Liste gegen die schriftliche Versicherung ausgehändigt, dass Namen, Adressen und sonstige Daten nicht zu anderen Zwecken Verwendung finden.

§ 5 Veröffentlichungen durch den BWK

(1) Von den Mitgliedern des Präsidiums, den Mitgliedern der Fachausschüsse sowie bestimmten Funktionsträgern kann für die Dauer der Übernahme der Tätigkeit, die Funktion, Name und Vorname, eine von den Personen selbst bestimmte Kontaktadresse und Kommunikationsdaten sowie eine Portraitfoto im Internet oder in gedruckter Form veröffentlich werden. Einer Veröffentlichung der Adress- und Kommunikationsdaten sowie des Portraitfotos kann jederzeit schriftlich widersprochen werden.

(2) Mit der Mitgliedschaft im BWK willigt das Mitglied ein, dass der Vereinsname, die Mitgliedsnummer sowie die vom Verein selbst bestimmten Kontaktadressen und Kommunikationsdaten veröffentlich werden. Funktionsträger des Mitglieds willigen mit Übernahme eines Amtes / einer Funktion ein, dass der Name, Vorname, die Kontaktadresse und von ihnen bestimmten Kommunikationsdaten vom BWK veröffentlich werden können. Die Veröffentlichung erfolgt in gedruckter Form sowie im Internet auf den Webseiten des BWK. Diese Einwilligung in die Veröffentlichung kann von der betroffenen Person jederzeit widerrufen werden.

(3) Der BWK veröffentlicht Informationen über besondere Ereignisse und sportliche Ergebnisse der Verbandstätigkeit, insbesondere die Durchführung und die Ergebnisse von Turnieren, auf der offiziellen Webseite des BWK sowie in der Verbandszeitschrift. Dabei können personenbezogene Daten veröffentlich werden. Von den persönlichen Daten sind dabei nur Name, Vorname, Vereinzugehörigkeit und - soweit notwendig - die Angabe der Alterskategorie zu veröffentlichen. Das einzelne Mitglied kann jederzeit gegenüber dem Präsidium Einwände gegen eine solche Veröffentlichung seiner Daten vorbringen. In diesem Fall unterbleibt in Bezug auf dieses Mitglied eine weitere Veröffentlichung mit Ausnahme von Ergebnissen aus dem Turnierbetrieb.

(4) Bei der Veröffentlichung im Internet sind ausreichend technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen. Dennoch kann bei einer Veröffentlichung von personenbezogenen Daten im Internet ein umfassender Datenschutz nicht garantiert werden, da die personenbezogenen Daten auch in Staaten abrufbar sind, die keine der Bundesrepublik Deutsch-

land vergleichbaren Datenschutzbestimmungen kennen und somit die Vertraulichkeit, die Integrität (Unverletzlichkeit), die Authentizität (Echtheit) und die Verfügbarkeit der personenbezogenen Daten im Internet nicht gesichert ist.

§ 6 Auftragsdatenverarbeitung

(1) Der BWK beauftragt andere Unternehmen und Einzelpersonen mit der Erfüllung von Aufgaben. Beispiele sind u.a. der Betrieb der Internetpräsenz und die Abwicklung von Zahlungen (Lastschriftverfahren). Diese Dienstleister haben Zugang zu persönlichen Informationen, die zur Erfüllung ihrer Aufgabe benötigt werden.

(2) Diese Auftragsdatenverarbeiter nach Weisung des BWK sind im Verhältnis zum BWK datenschutzrechtlich als Auftragsnehmer und nicht als Dritte anzusehen (§ 3 Abs. 8 Satz 3 BDSG). Die im Rahmen dieses Service vorgenommene Datenverarbeitung oder -nutzung ist dem BWK zuzurechnen (§ 11 Abs. 1 BDSG).

(3) Die Einzelheiten der Auftragsdatenverarbeitung - insbesondere die Festlegung, welche Daten für welche Zwecke verarbeitet oder genutzt werden dürfen, sowie die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG und der Anlage hierzu - sind durch einen schriftlichen Vertrag zwischen dem BWK und der Servicestelle festzulegen (§ 11 Abs. 2 Satz 2 BDSG). Dabei ist eine Nutzung bzw. Übermittlung über den vereinbarten Zweck (s. Abs. 1) hinaus vertraglich auszuschließen und die sichere Vernichtung bzw. Rückgabe der Daten zu vereinbaren.

§ 7 Datensperrung und -löschung

(1) Daten von Mitgliedern, Präsidiumsmitgliedern und Funktionsträgern werden nach Austritt aus dem Verband bzw. Beendigung der Tätigkeit gelöscht, sobald ihre Kenntnis nicht mehr erforderlich ist.

(2) Daten die einer gesetzlichen oder satzungsmäßigen Aufbewahrungsfrist unterliegen, werden für die weitere Verwendung gesperrt und nach Ablauf der Aufbewahrungspflicht entsprechend Abs. 1 gelöscht.

§ 8 Organisatorisches

(1) Für die Einhaltung des Datenschutzes ist der BGB-Vorstand des BWK verantwortlich. Diese Aufgabe kann innerhalb des geschäftsführenden Präsidiums delegiert werden (§ 4g Abs. 2a BDSG)

(2) Alle Personen, die Zugang zu personenbezogenen Daten haben, insbesondere die Funktionsträger des Verbandes, sind schriftlich auf die Wahrung des Datengeheimnisses zu verpflichten (§ 5 BDSG).

(3) Um die Aktualität der gemäß § 1 Abs. 4 erfassten Daten zu gewährleisten, sind die Mitgliedsvereine, Präsidiumsmitglieder und Funktionsträger verpflichtet, Veränderungen umgehend dem BWK-Präsidium oder einem vom Präsidium des BWK mit der Datenverarbeitung beauftragten Dritten mitzuteilen.

(4) Die Mitglieder des BWK verpflichten sich, ihre Mitglieder über das BDSG zu informieren und ihnen ihre Rechte und Pflichten zu erläutern.

(5) Zur Überwachung der Datenschutzbestimmungen wird vom Präsidium des BWK ein Datenschutzbeauftragter bestellt. Er muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen.

(6) Dieser ist dem Präsidium unmittelbar unterstellt, auf dem Gebiet des Datenschutzes ist er bei Anwendung seiner Fachkunde weisungsfrei.

(7) Der Datenschutzbeauftragte kontrolliert die Einhaltung des Datenschutzes im Verband. Er hat über seine Tätigkeit auf Antrag zu berichten.

§ 9 Inkrafttreten und Bekanntgabe

Diese Datenschutzordnung wurde in der Hauptversammlung des BWK am 24.10.2015 mit Mehrheit beschlossen.

Begriffserklärungen und Definitionen

Informationelles Selbstbestimmungsrecht

Das Informationelle Selbstbestimmungsrecht bezeichnet allgemein die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dieses Recht wurde in Deutschland vom Bundesverfassungsgericht im Volkszählungsurteil als Grundrecht anerkannt, das sich aus den Artikeln 1 und 2 Grundgesetz ergibt. Im Gegensatz zum Grundgesetz wurde das Informationelle Selbstbestimmungsrecht in eine Reihe von Landesverfassungen ausdrücklich aufgenommen.

Im Einzelnen beschreibt das Bundesverfassungsgericht dieses Recht wie folgt:

"Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Artikel 2 Abs. 1 in Verbindung mit Artikel I Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Personenbezogene Daten

Personenbezogene Daten stellen allgemein die Gesamtheit aller Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person" im Sinne des Datenschutzes) dar. Als bestimmbar wird in diesem Zusammenhang eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Element/en, das/die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität ist/sind.

Der Personenbezug ist der zentralste aller Begriffe im Datenschutz. Nahezu alle Datenschutzvorschriften gelten ausschließlich für personenbezogene Daten. Daher hat es auch nicht an Versuchen gefehlt, bestimmten Daten, die nur mittelbar mit einer Person zu tun haben, den Personenbezug abzusprechen. Literatur und Rechtsprechung sind dem in aller Regel jedoch nicht gefolgt.

Die maßgebliche Definition des Begriffs ist in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) enthalten. Auf ihn nehmen andere Datenschutzgesetze entweder Bezug, oder er wird dort mehr oder weniger wörtlich wiederholt. Demnach sind personenbezogene Daten

- Einzelangaben
- über persönliche und sachliche Verhältnisse
- einer bestimmten oder bestimmbaren natürlichen Person.

Die Daten juristischer Personen (GmbH, Aktiengesellschaft usw.) sind also nicht erfasst. Die Bedeutung der anderen Definitionskriterien lautet wie folgt:

- "Bestimmt" wird eine Person in der Regel dadurch, dass sie direkt namentlich genannt ist.
- "Bestimmbar" wird sie u.a. dadurch, dass man sie mithilfe der vorhandenen Angaben bestimmen kann, wenn man öffentlich zugängliche Quellen (Telefonbuch, aber z.B. auch Handelsregister) hinzuzieht. Dieses weite Verständnis des Begriffs "Bestimmbar" führt dazu, dass eine Bestimmbarkeit in der Praxis sehr häufig gegeben ist.
- "Einzelangaben" sind alle Angaben, die etwas über eine Person aussagen, also im Ergebnis nahezu alles.
- "persönliche oder sachliche Verhältnisse" decken alles ab, was sich auf eine Person bezieht, von der Wirtschaftslage über den Familienstand bis hin zu verwandtschaftlichen Verflechtungen (z.B. auch Ehrungen, Mitgliedschaft in Organisationen und dergleichen.

Nicht vom Bundesdatenschutzgesetz geschützt werden Angaben über Verstorbene (bspw. in einem Nachruf für ein verstorbenes Mitglied in den Verbandsmedien).

Verantwortliche Stelle

Im Sinne des § 3 des Bundesdatenschutzgesetzes (BDSG) jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Der Bund Westfälischer Karneval ist die für die Mitgliederdaten verantwortliche Stelle (§ 3 Abs. 7 BDSG).

Funktionsträger

Funktionsträger des BWK sind gewählte Mitglieder der satzungsmäßigen Organe und Personen, die sonstige in der Satzung genannte Ämter oder Aufgaben ausüben bzw. erfüllen. Beauftragte des BWK, z.B. sonstige ehrenamtliche Mitarbeiter/innen in Arbeitsgruppen, die namentlich benannt sind.

Datenerhebung

Erheben ist das Beschaffen von Daten über den Betroffenen. Es bedarf einer Aktivität, durch die die erhebende Stelle oder Person Kenntnis von den Daten erhält oder die Verfügung über diese begründet.

Beschaffen von Daten

Erheben bedeutet das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG). Das kann auf ganz unterschiedliche Weise geschehen:

- Aushändigung eines Formulars an den Betroffenen mit der Bitte, es auszufüllen
- Erfragen von Informationen beim Betroffenen
- Erfragen von Informationen über den Betroffenen

Varianten des Vorgehens

Grundlegend zu unterscheiden sind hinsichtlich der Erhebung folgende Begriffspaare:

- Erhebung beim Betroffenen/bei einem Dritten
- Zwangsweise Erhebung/freiwillige Erhebung
- Offene Erhebung/verdeckte Erhebung

Die Erhebung von Daten bedarf durchweg einer Rechtsgrundlage. Dies gilt für öffentliche und nicht-öffentliche Stellen gleichermaßen.

Datenverarbeitung

Das Verarbeiten von Daten ist ein Teil des Umgangs mit Daten. Es umfasst fünft weitere Begriffe (s. § 3 Abs. 4 BDSG), nämlich

- Speichern
- Verändern
- Übermitteln (Übermittlung)
- Sperren (Sperrung)
- Löschen (Löschung)

An dem Begriff der Verarbeitung knüpft das Gesetz vor allen Dingen dann an, wenn es die fünf weiteren Begriffe, die sich hinter ihm verbergen, sozusagen "auf einmal" erfassen will.

Datenspeicherung

"Speichern" bedeutet als Datenverwendung das Vorrätig-Halten von Daten in elektronischen Dateien und in Akten, soweit die Akten so strukturiert sind, dass ein gezielter Zugriff auf personenbezogene Daten möglich wird. Der Begriff ist also nicht allein im elektronischen Sinne zu verstehen.

Darüber hinaus bedeutet "Speichern" das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung

Datenveränderung

Verändern bezieht sich auf das inhaltliche Umgestalten gespeicherter personenbezogener Daten (z.B. Änderung des Ansprechpartners, Korrektur fehlerhafter Eingaben, Veränderung von Daten).

Datenübermittlung

Im Sinne des Datenschutzes ein Vorgang, bei dem die speichernde Stelle gespeicherte oder durch Datenverarbeitung gewonnene personenbezogener Daten an einen Dritten in der Weise weitergibt, dass der Dritte Einsicht erhält oder die Daten dann für ihre eigenen Zwecke nutzen und verarbeiten kann. Die Übermittlung unterliegt den Vorschriften des Datenschutzes in §§ 16 - 18 sowie 28 und 29 des Bundesdatenschutzgesetzes.

Daten sperren

Gesperrte Daten sind noch vorhanden, dürfen aber nicht mehr verarbeitet oder genutzt werden. Um dies sicherzustellen, werden sie entsprechend gekennzeichnet (§ 3 Abs. 4 Nr. 4 BDSG). Dass die Daten nach wie vor vorhanden sind, unterscheidet die Sperrung von der Löschung.

Ein Anspruch auf Sperrung besteht nicht ohne weiteres, weil es der Betroffene so möchte. Vielmehr müssen bestimmte, im Gesetz näher definierte Voraussetzungen erfüllt sein. Dabei ist zu unterscheiden zwischen

- den Fällen, in denen die Sperrung an die Stelle einer – aus irgendwelchen Gründen nicht möglichen – Löschung tritt (§ 20 Abs. 3 BDSG, § 35 Abs. 3 BDSG) und
- den Fällen, in denen die Richtigkeit von Daten umstritten ist und deshalb eine Sperrung erfolgt, bis diese Frage geklärt werden kann (§ 20 Abs. 4 BDSG, § 35 Abs. 4 BDSG).

Wie die Sperrung realisiert wird, lässt das Gesetz im Einzelnen offen. Unter dem Begriff "Kennzeichnen" lässt sich alles Mögliche verstehen. Diese Offenheit des Gesetzes ist angesichts des ständigen technischen Wandels sehr vernünftig. Entscheidend ist das Ergebnis: Die weitere Verarbeitung und Nutzung muss zuverlässig verhindert werden.

Daten löschen

Personenbezogene Daten, die für den rechtmäßigen Verwendungszweck nicht mehr gebraucht werden oder die rechtswidrig erhoben worden sind, müssen kraft Gesetzes gelöscht werden.

Deshalb verlangt der gesetzliche Begriff des Löschens eine Maßnahme, die unwiederbringlich dazu führt, dass die Informationen nicht mehr lesbar gemacht werden können. Eine Diskette kann beispielsweise manuell zerstört werden, und eine Festplatte ist sicher zu überschreiben.

Es ist zu beachten, dass aus Gründen der Datensicherheit Daten in Sicherungsdateien und Spiegelungen dupliziert vorhanden sind. Solche Datensicherungssysteme sind datenschutzgerecht so zu organisieren, dass ohne große zeitliche Verzögerung der Löschungspflicht, auch hier in der Regel automatisiert, nachgekommen wird.

Datennutzung

Unter Datennutzen ist jede Verwendung personenbezogener Daten zu verstehen, soweit es sich nicht um Verarbeitung handelt.

Daten anonymisieren

Im Sinne des Bundesdatenschutzgesetzes (BDSG) 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.

Daten pseudonymisieren

Im Sinne des Bundesdatenschutzgesetzes (BDSG) ist die Pseudonymisierung oder das Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wiederherstellen zu können. Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo Anonymisierung nicht möglich ist.

Automatisierte Verarbeitung

Automatisierte Verarbeitung 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 und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Zweckbindung

Im Datenschutz ein Schutzziel, das gewährleisten soll, dass personenbezogene Daten, die zu einem bestimmten Zweck erhoben wurden, nicht für andere Zwecke verwendet werden dürfen, es sei denn, der Betroffene hat zugestimmt.

Angesichts der intensiven Datenbearbeitungen, die bei den heutigen elektronisch vernetzten Informationssystemen anfallen, ist die Gefahr groß, dass Daten für einen anderen als den ursprünglich vorgesehenen Zweck verwendet werden. Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, der bei der Erhebung angegeben wurde.

Grundsatz der Erforderlichkeit

Hierbei handelt es sich um einen Rechtsbegriff, der an verschiedenen Stellen im BDSG auftritt. Er bringt allgemein zum Ausdruck, dass Maßnahmen, die in die Rechte des Betroffenen eingreifen, voraussetzen, dass die Maßnahmen unabdingbar sein müssen, um einen bestimmten Zweck zu erreichen, und keine gleichermaßen wirksame Maßnahme zur Verfügung steht.

Damit genügt nicht, dass eine Maßnahme einem Zweck (Zweckbindung) bloß dienlich ist. Es muss vielmehr dargelegt und bewiesen werden können, dass ohne die Maßnahme der Zweck nicht erreicht werden kann und eine zumutbare Alternative nicht besteht.

Einwilligung der betroffenen Person

Im Sinne der Europäischen Datenschutzrichtlinie (95/46/EG) vom 24. Oktober 1995 jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

Nach den Grundsätzen des Datenschutzes ist für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten entweder eine dies ausdrücklich erlaubende Rechtsvorschrift oder die Einwilligung des Betroffenen erforderlich. Nach § 4a BDSG muss die Einwilligung auf einer freien Entscheidung des Betroffenen beruhen. Der Betroffene muss vor der Einwilligung von der verarbeitenden Stelle auf den Zweck der Erhebung, Nutzung oder Verarbeitung hingewiesen werden.

Die Einwilligung muss grundsätzlich schriftlich erfolgen. Die Einwilligung muss im Text besonders hervorgehoben werden, wenn sie mit anderen Erklärungen zusammen erteilt werden soll.

Der Betroffene hat das Recht, seine Einwilligung jederzeit ganz oder teilweise zu widerrufen. Mit dem Zugang des Widerrufs dürfen die betreffenden Daten nicht mehr verwendet werden.

Betroffener

Der Begriff hat – ohne dass dies auf den ersten Blick deutlich wird – eine entscheidende Bedeutung für die Frage, ob Datenschutzvorschriften überhaupt zur Anwendung kommen. Von wenigen Ausnahmen abgesehen, beziehen sich Datenschutzvorschriften auf personenbezogene Daten. Das können nur Daten einer "bestimmten oder bestimmbaren natürlichen Person" sein. Diese Person heißt Betroffener (§ 3 Abs. 1 BDSG). Anders ausgedrückt: Wenn es keinen Betroffenen gibt, gibt es auch keine personenbezogenen Daten.

Es gibt auch Fälle der "Gruppenbetroffenheit". Bei ihnen geht es vordergründig um Daten einer Gruppe, also nicht Daten eines Einzelnen. Hat jedoch jedes Mitglied der Gruppe einen erkennbaren Anteil an der Leistung der Gesamtgruppe, dann beziehen sich die Daten über die Leistung nicht mehr auf die Gruppe insgesamt, sondern auch auf jedes einzelne Gruppenmitglied. Jedes Mitglied der Gruppe ist also Betroffener.

Empfänger

Empfänger ist jede Person oder Stelle, die Daten erhält, folglich auch innerhalb der Organisation.

Dritter

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte ist auch nicht der Betroffene.

Rechte des Betroffenen

Die allgemeine Zielsetzung des Datenschutzes, den Betroffenen vor Beeinträchtigungen seines Persönlichkeitsrechts zu schützen (§ 1 Abs. 1 BDSG), wird dadurch umgesetzt, dass dem Betroffenen in gesetzlichen Vorschriften einzelne konkrete Rechte eingeräumt werden. Dabei gibt es wichtige Rechte, die nicht in den allgemeinen Datenschutzgesetzen (BDSG und LDSGe) enthalten sind, sondern in anderen gesetzlichen Regelungen. Ein Beispiel dafür ist das Recht am eigenen Bild, das im Kunsturhebergesetz geregelt ist

Das BDSG regelt die Rechte des Betroffenen gegenüber Stellen des des nicht-öffentlichen Bereichs in unterschiedlichen Vorschriften:

- Recht auf Auskunft (§ 34 BDSG)
- Recht auf Berichtigung (§ 35 BDSG)
- Recht auf Löschung (§ 35 BDSG)
- Recht auf Sperrung (§ 35 BDSG)

Die bisher genannten Rechte sind gemäß einer ausdrücklichen gesetzlichen Regelung (§ 6 Abs. 1 BDSG) "unabdingbar". Dies bedeutet, die Rechte können weder durch Vertrag noch durch einseitige Erklärung des Betroffenen ausgeschlossen oder beschränkt werden.

Neben den Ansprüchen auf Auskunft, Benachrichtigung, Berichtigung, Sperrung und Löschung haben Betroffene Schadensersatzansprüche, wenn ihnen durch eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten ein Schaden entstanden ist.

Verursachen nicht öffentliche Stellen einen Schaden, enthält das BDSG diesbezüglich keine Anspruchsnorm. Deshalb sind die Vorschriften der §§ 823 ff. BGB anzuwenden, die immer ein Verschulden voraussetzen. Allerdings regelt das BDSG in § 7 eine Beweiserleichterung zugunsten des Betroffenen. Er muss nämlich ein Verschulden einer nicht öffentlichen Stelle nicht beweisen, sondern die nicht öffentliche Stelle muss sich entlasten, also beweisen, dass sie den entsprechenden Schaden nicht verschuldet hat.

Datengeheimnis

Allgemein die Kenntnis vom Vorhandensein und/oder Informationsinhalt von Daten, die auf eine bestimmte Person oder einen bestimmten Personenkreis beschränkt ist. Damit verbindet sich in der Regel die Verpflichtung, diese Kenntnis nicht gegenüber Dritten preiszugeben.

Nach dem Bundesdatenschutzgesetz haben Organisationen die Pflicht, ihre Mitarbeiter, soweit diese bei der Verarbeitung personenbezogener Daten beteiligt sind, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Datensparsamkeit

Im Datenschutz allgemein das Gebot zur Vermeidung nicht benötigter personenbezogener Daten.

Nach dem deutschen Bundesdatenschutzgesetz gilt u.a. der Grundsatz der Datensparsamkeit und Datenvermeidung. Danach dürfen nicht mehr Informationen, als für den erstrebten Zweck erforderlich sind, über eine Person erhoben und verwendet werden. Datenverarbeitungssysteme sollen von vornherein so gestaltet werden, dass dieser Grundsatz beachtet wird.

Auftragsdatenverarbeitung

Eine Übermittlung von Daten setzt nach dem BDSG in der Regel einen besonderen Rechtfertigungsgrund (Erlaubnistatbestand), beispielsweise eine Einwilligung, voraus. Eine Ausnahme gilt für die so genannte Auftragsdatenverarbeitung. In diesem Fall liegt keine Übermittlung von Daten an den Auftragnehmer vor, sondern die Verarbeitung durch den Auftragnehmer ist datenschutzrechtlich als eine Datenverarbeitung des Auftraggebers anzusehen. Durch diesen juristischen Kunstgriff werden die personenbezogenen Daten daher vom Auftragnehmer nicht im eigenen Namen, sondern im Namen des Auftraggebers verarbeitet. Das Privileg der Auftragsdatenverarbeitung führt dazu, dass der Auftragnehmer datenschutzrechtlich annähernd wie eine bloße Abteilung des Auftraggebers zu betrachten ist.

Der Auftragnehmer ist nach § 11 BDSG nur dafür verantwortliche, dass hinreichende technische und organisatorische Maßnahmen der Datensicherheit eingehalten werden (begrenzte datenschutzrechtliche Pflichten). Die Verantwortung für die Einhaltung aller weiteren Pflichten nach dem BDSG verbleibt beim Auftraggeber. Der Auftragnehmer darf die Daten nur im Rahmen der klaren Weisungen des Auftraggebers verarbeiten und nutzen.

Datenschutzrechtlich trifft den Auftragnehmer noch eine Nebenpflicht. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, so hat er den Auftraggeber unverzüglich auf dessen möglichen Verstoß hinzuweisen. Die Erfüllung datenschutzrechtlicher Pflichten verbleibt aber auch in diesem Fall beim Auftraggeber. Der Auftragnehmer tritt nicht in dessen datenschutzrechtliche Pflichten ein, sondern ist nur für die Datensicherheit verantwortlich.

Der Auftraggeber ist verpflichtet, den Auftragnehmer sorgfältig auszuwählen. Er hat darauf zu achten, dass der Auftragnehmer die Datensicherheitsanforderungen erfüllen kann. Der Auftragnehmer muss ein schriftliches Datensicherheitskonzept haben.

Der Vertrag über die Auftragsdatenverarbeitung hat folgende Voraussetzungen zu erfüllen:

- Der Vertrag muss schriftlich vorliegen, also eigenhändig von den Parteien unterzeichnet sein. Eine Vertretung, insbesondere innerhalb von Konzernen, ist möglich.
- Der Vertrag muss genau benennen, welche Daten weitergegeben und wie sie verarbeitet und genutzt werden sollen.
- Der Vertrag hat die beim Auftragnehmer tatsächlich vorhandenen technischen und organisatorischen Maßnahmen der Datensicherheit aufzuzeigen. Dabei kann insbesondere auf das Datensicherheitskonzept des Auftragnehmers Bezug genommen werden.
- Der Vertrag muss festlegen, ob und unter welchen Voraussetzungen Unterauftragnehmer eingeschaltet werden dürfen.

Verfahrensverzeichnis

Jedes Unternehmen hat seine Verfahren automatisierter Verwendung von Daten mit bestimmten Angaben zu erfassen und in ein Verfahrensverzeichnis aufzunehmen, damit der betriebliche Datenschutzbeauftragte bzw. die Aufsichtsbehörde die Problempunkte erkennen kann, bei denen aus Sicht des Datenschutzes Handlungsbedarf bestehen könnte.

In das Verfahrensverzeichnis müssen folgende Angaben aufgenommen werden:

- der handelsrechtlich korrekte Name des Unternehmens
- Angaben über den Inhaber oder Geschäftsleiter des Unternehmens sowie den IT-Leiter
- die Anschrift des Unternehmens
- die einzelnen Zwecke der Datenerhebung und -verwendung, also die verschiedenen Verfahren der Datenverwendung
- eine gattungsmäßige Beschreibung der Personen, deren Daten verwendet werden (beispielsweise Interessenten), und der von ihnen erhobenen und zu verwendenden Daten
- die möglichen Empfänger, denen die Daten mitgeteilt werden sollen
- die Frist, in denen die Daten mit Rücksicht auf gesetzliche Vorschriften wieder gelöscht werden sollen
- eine geplante Datenübermittlung in Drittstaaten, also in Länder außerhalb der EU und des EWR
- eine allgemeine Beschreibung, die es ermöglicht zu beurteilen, ob die Datensicherheitsmaßnahmen (Datensicherung) angemessen sind.

Mit dem Begriff des öffentlichen Verfahrensverzeichnisses ist auf den Umstand verwiesen, dass die Angaben des Verfahrensverzeichnisses von Ziffer 1 bis 8 auf Anfrage jedermann zugänglich gemacht werden müssen.

Haftung

Unter Haftung versteht man im Allgemeinen, dass jemand für einen entstandenen Schaden einstehen muss. Insofern ist der Begriff äußerst allgemein.

Im Datenschutz kommt eine Haftung unter ganz verschiedenen Aspekten in Betracht:

- Haftung der verantwortlichen Stelle gegenüber dem Betroffenen
  Sie ist z.B. denkbar, wenn Daten rechtswidrig übermittelt werden und dem Betroffenen hieraus ein Schaden entsteht (s. § 7 und § 8 BDSG).
- Haftung des Auftragnehmers bei einer Auftragserhebung, -verarbeitung, -nutzung
  Sie ist dann denkbar, wenn sich der Auftragnehmer über Anweisungen des Auftraggebers hinweg-setzt und es dadurch zu einem Schaden kommt.
- Haftung des Datenschutzbeauftragten
  Sie ist dann denkbar, wenn der Datenschutzbeauftragte seine Pflichten nicht erfüllt und es dadurch bei der Stelle, für die er tätig ist, oder beim Betroffenen zu einem Schaden kommt.

Datensicherheit

Allgemein der Zustand, bei dem Daten im Prozess der Datenverarbeitung und ggf. des Datentransports vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung geschützt sind. Daneben bezeichnet "Datensicherheit" auch die Aufgabe, Dateien und die Datenverarbeitung gegen Datenverlust, Datenzerstörung, Datenverfälschung und Datenpreisgabe zu schützen.

In Deutschland sind Unternehmen, Organisationen und Behörden gesetzlich verpflichtet, die notwendigen technischen und organisatorischen Maßnahmen zum Erreichen und Aufrechterhalten von Datensicherheit zu treffen, damit die Ordnungsmäßigkeit der Datenverarbeitung gesichert ist. Diese Maßnahmen erfordern mehr als die herkömmlichen Maßnahmen einer rein technischen Datensicherung, bei denen in der Regel nur die Absicherung der Integrität (Zugriffsrechte) und Reproduzierbarkeit der Daten (bei Verlust) im Vordergrund stehen.

Vielmehr muss gesichert sein, dass insbesondere

- nur Befugte Zugriff auf die Daten besitzen und diese zur Kenntnis nehmen können,
- die Daten inhaltlich korrekt sind und vom angegebenen Urheber stammen,
- nur Befugte die Daten in zulässiger Weise modifizieren (ändern, löschen) dürfen und möglichen Modifikationen der Daten durch technische Funktionsstörungen vorgebeugt wird,
- Befugte entsprechend ihren Rechten auf die Daten jederzeit zugreifen können und die Funktionalität des IT-Systems nicht beeinträchtigt ist,
- die Systeme revisionsfähig sind.

Das Bundesdatenschutzgesetz zählt in der Anlage zu § 9 Satz 1 bestimmte konkrete Maßnahmen der Datensicherheit auf, die jedoch nicht abschließend sind.

Bund Westfälischer Karneval e.V.
Geschäftsstelle
Postfach 1111
59701 Arnsberg
Tel. 02932 496254
E-Mail: geschaeftsstelle@bwk-online.de