Merkblatt zum Datenschutz

Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet!

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen des Bundesdatenschutzgesetzes [BDSG] beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT- Systemen und -Anwendungen sind die zentralen Zielsetzungen. Fehlverhalten kann zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Kundeneffekten führen.

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass durch den Umgang mit seinen personenbezogenen Daten seine Persönlichkeitsrechte beeinträchtigt werden.

Kernaussagen des Bundesdatenschutzgesetzes (BDSG)

Gültigkeit

Das Gesetz gilt u.a. für alle so genannten „nicht-öffentlichen Stellen“: das sind alle Unternehmen, Vereine oder sonstige Vereinigungen, aber auch Niederlassungen ausländischer Unternehmen unabhängig von der Rechtsform. Die gesetzlichen Regelungen betreffen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.

Begriff Personenbezogene Daten (§ 3 Abs. 1 BDSG)

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, gleichgültig ob Mitarbeiter, Kollege oder Kunde bzw. Lieferant oder deren Ansprechpartner [Betroffener]. Also, alle Angaben, welche zu einer identifizierbaren Person gehören, z.B. Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse.

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, PC-Benutzerkennung, maschinenbezogene Nutzungszeiten bei nur einem in Frage kommenden Benutzer).

Ausnahmen vom Verbot, mit personenbezogenen Daten umzugehen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Die Daten müssen für die Zwecke, für die sie erhoben und verarbeitet werden z.B. im Rahmen eines Vertrages, relevant sein, sachlich richtig sein, und dürfen nur so lange gespeichert werden, wie es der genannte Zweck erfordert. Unrichtige oder unvollständige Daten sind zu löschen oder zu berichtigen. Nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine anderweitige Verarbeitung zulässig.

Einwilligung

Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung, sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf meistens der Schriftform, und ggf. ist eine optische Hervorhebung erforderlich. Für bestimmte Daten im Rahmen der Internet-Kommunikation ist auch eine elektronische Einwilligung zulässig. Die Einwilligung für besondere Kategorien personenbezogener Daten (=besonders sensitive Daten) ist gesondert erforderlich.

Begriff Besondere Kategorien

Besondere Kategorien personenbezogener Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben oder strafrechtliche Verurteilungen. Hier gelten besondere Vorschriften!

Rechte der Betroffenen

Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber der speichernden Stelle grundsätzlich das Recht auf Auskunft über gespeicherte Daten, Zweck und Rechtsgrundla-

ge der Speicherung sowie Herkunft und Empfänger von Übermittlungen. Unzutreffende Daten sind zu berichtigen, unzulässig gespeicherte oder nicht mehr erforderliche Daten zu löschen.

Wenn jemandem durch eine unrechtmäßige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt wird, ist ihm Schadenersatz zu gewähren.

Jedermann hat das Recht, sich unmittelbar an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt zu sein; dies gilt auch für Beschäftigte in Unternehmen.

Datensicherheit durch entsprechende technische und organisatorische Maßnahmen

Das Gesetz verlangt die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Obwohl üblicherweise Ihr Arbeitgeber die notwendigen Maßnahmen organisiert, ist jeder einzelne Mitarbeiter für die Umsetzung mit verantwortlich. Richtiges Verhalten gemäß Arbeitsvertrag und Arbeits-/Dienstanweisung ist unabdingbar. Einige ausgewählte Anforderungen sind im Folgenden dargestellt:

- **Zutritt**: Unbefugten ist der Zutritt zu den Rechneranlagen, Servern und PC, auf denen personenbezogene Daten verarbeitet werden, zu verwehren. Art und Umfang der notwendigen Sicherungsmaßnahmen zur Zutrittskontrolle richten sich nach der Sensibilität und der Menge der gespeicherten Daten.
- **Zugriff** auf Daten und Informationen in einem Netzwerk oder auf EDV-Anlagen/PC darf nur berechtigten Personen ermöglicht werden. Durch Benutzerkennung und Passwort werden die Systeme durch den Arbeitgeber entsprechend geschützt. In Ihrer Verantwortung liegt aber der vertrauliche und sorgfältige Umgang mit Ihren Zugangsberechtigungsdaten (Passwort).
- **Weitergabe** von Daten und Informationen: Es ist sicherzustellen, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Obwohl zahlreiche betriebliche Vorkehrungen getroffen sind, bleiben Sie als Mitarbeiter auch für die Umsetzung dieser Vorschrift mit verantwortlich, Gefährdungen zu verhindern. Beispiele sind die Weitergabe von Disketten oder CD-ROM mit Daten.

Übermittlung in Nicht-EU/EWR-Staaten

Die Übermittlung in Nicht-EU/EWR-Staaten ist nur bei sehr beschränkten Ausnahmen zulässig.

Verpflichtung zur Wahrung des Datengeheimnisses

Allen Mitarbeitern, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten oder zu nutzen; dies gilt auch nach Beendigung Ihrer Tätigkeit. Deshalb wurden Sie gemäß § 5 BDSG auf die zu beachtenden Vorschriften über den Datenschutz verpflichtet.

Zuwiderhandlungen gegen das BDSG sind mit Bußgeld, Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe belegt.

Achtung! Folgender Text sollte nur bei Unternehmen der Kreditwirtschaft in das Merkblatt eingefügt werden.

Das **Bankgeheimnis** normiert die Verpflichtung des Kreditinstituts, einem Dritten gegenüber keinerlei Auskünfte über Konten und Depots seiner Kunden, sowie über sonstige, ihm aus der Geschäftsverbindung mit dem Kunden bekannt gewordene Tatsachen zu geben. Eine Ausnahme besteht nur dann, wenn das Kreditinstitut kraft Gesetzes zur Auskunft verpflichtet oder vertraglich zu ihrer Erteilung berechtigt ist. Das Bankgeheimnis schützt nicht nur natürliche Personen (wie der Datenschutz), sondern auch juristische Personen.

Allgemeine Verhaltensregeln beim Umgang mit Daten

Es gelten vorrangig die Dienstanweisungen Ihres Unternehmens!

- Nur sichere Passwörter auswählen (z.B. mit Sonderzeichen, keine Namen) und regelmäßig wechseln.

- Bildschirme und PC sind bei Abwesenheit vom Arbeitsplatz zu sperren.
- Laptops bei Reisen sorgfältig sichern, besonders im Auto, Hotel oder auf Flughäfen.
- Keine vertraulichen Informationen per Fax schicken, falls doch erforderlich, besondere Vorkehrungen treffen (z.B. telefonische Absprache wegen Anwesenheit des Empfängers, Doppelkontrolle der Richtigkeit der gewählten der eingegebenen Fax-Nummer vor Versand).
- Nicht einfach mit Antwortfunktion auf E-Mail mit vertraulichem Inhalt reagieren, vorher Absenderlisten überprüfen! (Achtung: vertrauliche Informationen über E-Mail grundsätzlich nicht versenden, wenn keine Verschlüsselung genutzt werden kann).
- Vertrauliche Telefonate nicht vom Handy in der Öffentlichkeit führen.

Bei Fragen zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wenden Sie sich bitte an Ihren Beauftragten für den Datenschutz.