Merkblatt zum Datenschutz und zum Fernmeldegeheimnis

Datenschutz ist ein **Grundrecht**. Er hat das Ziel, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem **Persönlichkeitsrecht** beeinträchtigt wird. Der Einzelne hat das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Das erfordert einen verantwortungsvollen Umgang mit personenbezogenen Daten, unabhängig davon, ob er mit oder ohne die Unterstützung von IT-Systemen erfolgt.

Es ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verwenden oder sonst zu verarbeiten.

1. Verpflichtung zum Datenschutz

Was sind personenbezogene Daten? Personenbezogene Daten sind Angaben über eine **bestimmte oder bestimmbare natürliche Person**. Beispiele: Name, Vorname, Berufsbezeichnung, Titel, Anschrift, Geburtstag, Bonitätsdaten, Kreditkartendaten, Prüfungsergebnisse, Gehalt, Vorlieben, Kaufverhaltensmerkmale. Angaben über juristische Personen – wie Firmen ohne Einzelinhaber – sind keine personenbezogenen Daten.

Was ist eine Datenverarbeitung? Der Begriff der Verarbeitung ist **umfassend** zu verstehen und beinhaltet viele verschiedene denkbare Verarbeitungsschritte. Sie beginnt bei der Beschaffung („Erhebung“) von Daten (direkt von der betroffenen Person oder bei Dritten), umfasst die Verwendung (z.B. Speicherung, Veränderung, Verknüpfung, Weitergabe) und auch ihre Löschung.

Wann ist die Datenverarbeitung erlaubt? Nach der **Datenschutzgrundverordnung** (DSGVO) bedarf jede Verarbeitung personenbezogener Daten einer gesetzlichen Grundlage. Die DSGVO selbst (Art. 6, 88) und auf ihrer Grundlage auch das Bundesdatenschutzgesetz (BDSG) und andere Rechtsvorschriften, z.B. Gesetze wie die Abgabenordnung, die Rechtspflichten zur Datenverarbeitung enthalten, oder Betriebsvereinbarungen formulieren solche Erlaubnisgründe. Erlaubt ist z. B. die Verwendung personenbezogener Daten, wenn dies im Rahmen eines rechtsgeschäftlichen oder eines rechtsgeschäftsähnlichen Schuldverhältnisses (z. B. zur Durchführung der Kundenbeziehung oder des Beschäftigungsverhältnisses) erforderlich ist oder aufgrund einer Einwilligung des Betroffenen. Die Verwendung personenbezogener Daten ist aber auch gemäß DSGVO zulässig, soweit diese zur Wahrung berechtigter Unternehmensinteressen erforderlich ist und kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen der Betroffenen (z. B. von Beschäftigen oder Kunden) überwiegen.

Für den Umgang mit Personalaktendaten von Beamten sind abschließende Sonderregelungen des Bundesbeamtengesetzes und der Personalaktenrichtlinie des BEV zu beachten. Danach sind die Personalaktendaten vertraulich zu behandeln und durch technische und organisatorische Maßnahmen vor unbefugter Einsichtnahme zu schützen.

Welche Rechte haben betroffene Personen? Die Datenverarbeitung soll für jeden Mitarbeiter, Kunden oder sonstige betroffene Personen transparent und überprüfbar sein. Die DSGVO gibt daher den von der Datenverarbeitung betroffenen Personen u. a. folgende Rechte:

- **Information:** Bereits bei Erhebung von Daten bei der betroffenen Person oder möglichst zeitnah im Zusammenhang mit der Erhebung bei Dritten, ist die betroffene Person u.a. über die Zwecke der Verarbeitung, über mögliche Empfänger, die Speicherdauer und über ihre Rechte zu informieren.
- **Auskunft:** Die betroffene Person hat das Recht zu erfahren, welche Daten verarbeitet werden, wo sie herkommen, zu welchem Zweck die Speicherung erfolgt und auch auf namentliche Nennung der Personen und Stellen, die seine Daten erhalten.
- **Berichtigung, Löschung, Einschränkung der Verarbeitung und Recht auf Vergessenwerden:** Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder diese nicht mehr erforderlich ist. Einer Löschung stehen allerdings oft z. B. rechtliche Aufbewahrungsfristen (aus Handelsgesetzbuch oder Abgabenordnung) entgegen. Hier sieht das Gesetz eine Einschränkung der Verarbeitung („Sperrung“) statt der Löschung vor. Die betroffene Person ist hierüber zu informieren.
- **Datenübertragung:** Hat die betroffene Person Daten z.B. in einem sozialen Netzwerk oder Kundenkonto bereitgestellt, kann sie verlangen, diese in einem maschinenlesbaren Format an sie selbst oder an einen Dritten zu übertragen.
- **Widerspruch gegen Werbung sowie eigene Markt- und Meinungsforschung:** Der Kunde hat ein Recht auf Widerspruch gegen Werbung und Markt- und Meinungsforschung. Auf dieses Widerspruchsrecht ist der Kunde bei einem Vertragsschluss und der Ansprache zu vorgenannten Zwecken stets hinzuweisen. Der Hinweis auf das Widerspruchsrecht muss zwingend den Adressaten und dessen Kontaktdaten enthalten. Wird ein Widerspruch erklärt, gilt er grundsätzlich unbeschränkt. Einwilligungen werden durch einen unbeschränkten Widerspruch wirkungslos.

Welche Datensicherheitsmaßnahmen können zur Vorbeugung von Datenschutzverstößen getroffen werden? Das Datenschutzrecht fordert geeignete und angemessene Maßnahmen zur Gewährleistung der Sicherheit personenbezogener Daten. Auch Sie können beim Umgang mit Daten dazu beitragen, dass diese vor unberechtigten Zugriffen geschützt werden. Solche Maßnahmen können unter anderem sein:

Vertraulichkeit	**Zutrittskontrolle:** Unbefugten ist der räumliche Zutritt zu Datenverarbeitungsanlagen zu verwehren. Dies kann z.B. durch Schlüssel, Chipkarten, Werksschutz, Pförtner erreicht werden.
	Zugangskontrolle: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, z.B. durch Vergabe von persönlichen Passwörtern, Verschlüsselung von Datenträgern.
	Zugriffskontrolle: Es ist zu gewährleisten, dass (systemische) Datenzugriffsmöglichkeiten nur im Umfang von Befugnissen und Erforderlichkeiten bestehen. Dieses Ziel kann z.B. durch ein Rollen- und Berechtigungskonzept, durch eine Verschlüsselung oder durch Protokollierung von Zugriffen erreicht werden.
	Weitergabekontrolle: Es ist zu gewährleisten, dass auf personenbezogene Daten bei Übertragung, Transport oder auf Datenträgern nicht unbefugt zugegriffen und dass festgestellt werden kann, welchen Stellen die Daten offengelegt wurden. Dies kann z.B. durch Verwendung sicherer Transportbehälter für Datenträger, VPN oder durch eine Verschlüsselung sichergestellt werden.
Integrität	**Eingabekontrolle:** Es ist zu gewährleisten, dass festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet wurden. In Betracht kommt hier z.B. eine Protokollierung der eingegebenen Daten, Dokumentenmanagement.
	Datentrennung: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann durch den Einsatz einer Software zur Mandantentrennung erreicht werden.
Verfügbarkeit	**Verfügbarkeitskontrolle:** Es ist zu gewährleisten, dass personenbezogene Daten gegen Verlust geschützt sind, was z.B. durch Backups, unterbrechungsfreie Stromversorgung, Virenschutz, oder Firewall erreicht werden kann.

Was ist bei einem Datenschutzverstoß zu tun? Wird Ihnen ein (möglicher) Datenschutzverstoß gewahr, dann informieren Sie bitte umgehend Ihren Auftraggeber.

2. Fernmeldegeheimnis

Für ein Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt, gilt das Fernmeldegeheimnis gemäß § 88 Telekommunikationsgesetz (TKG). Das Fernmeldegeheimnis verbietet es, die Inhalte und die näheren Umstände der Telekommunikation mehr als zum Zweck des Erbringens des Telekommunikationsdienstes erforderlich ist, zur Kenntnis zu nehmen und die Kenntnisse anderweitig zu verwenden. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Vom Fernmeldegeheimnis geschützt wird auch die Tatsache, ob jemand (natürliche oder juristische Person, § 91 TKG) an einem Telekommunikationsvorgang beteiligt ist oder war. Vom Fernmeldegeheimnis umfasst sind dabei nicht nur Telefonate und Faxe, sondern grundsätzlich auch die E-Mailkommunikation.

3. Straf- und Bußgeldvorschriften

Verstöße gegen den Datenschutz und das Fernmeldegeheimnis können mit Geld- und Freiheitsstrafe geahndet werden.