Verpflichtung auf die Wahrung der Vertraulichkeit und Integrität
bei der Verarbeitung personenbezogener Daten

Personenbezogene Daten sind nach den gesetzlichen Vorschriften so zu verarbeiten, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer personenbezogenen Daten gewährleistet werden. Dies umfasst jeglichen Umgang mit Daten, die zu einer identifizierten oder identifizierbaren natürlichen Person in Bezug stehen.

- Daher ist es Ihnen nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder fahrlässig die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zu unbefugter Offenlegung oder unbefugtem Zugang führt.

- Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden.
- Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.
- Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend arbeitsrechtlich geahndet werden kann.

Soweit Sie im Bereich der EDV bzw. Betreuung/Administration der Telekommunikationsanlage arbeiten, berührt Ihre Tätigkeit evtl. das Fernmeldegeheimnis. Sie dürfen sich für diesen Fall nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Sie dürfen derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung der Tätigkeit uneingeschränkt fort.

Ich habe mit meiner Onlinezustimmung erklärt, die Vertraulichkeit und Integrität personenbezogener Daten gemäß den oben beschriebenen Vorgaben einzuhalten.

–

Eine Verletzung datenschutzrechtlicher und anderer Vorschriften **kann mit Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** geahndet werden. Entsprechende Vorschriften können sich z.B. aus Art. 84 DSGVO i.V.m. § 42 BDSG-neu, § 17 UWG, § 202a Abs. 1 StGB, § 303a Abs. 1 StGB, § 88 TKG, § 78 Abs. 1 Satz 2 & 3 SGB X, § 203 StGB ergeben. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Erläuterungen und Verhaltenshinweise zum Datenschutz

Zielsetzung des Datenschutzrechts
Der Mensch (= **betroffene Person**) soll vor den möglichen Gefahren geschützt werden, die sich aus der bloßen Datenverarbeitung oder aus der Nutzung seiner Daten für das grundgesetzlich verbürgte **Persönlichkeitsrecht** ergeben können.
Datenschutz = Schutz des Menschen.
Datensicherung = Schutz der Daten.

Der Begriff "Personenbezogene Daten"
Personenbezogene Daten sind Informationen jedweder Art zu einer identifizierten oder identifizierbaren natürlichen Person, gleichgültig ob Mitarbeiter, Kollege, Kunde bzw. Lieferant oder Ansprechpartner. Jede Information zu einer dieser Personen zählt dazu: also auch bereits die Telefonnummer oder die E-Mail-Adresse; ebenso der Inhalt einer E-Mail. Auch wenn es sich um Einzelgewerbetreibende oder Freiberufler handelt, ist ein Personenbezug grundsätzlich anzunehmen.
Gehen Sie im Zweifel bei Daten immer davon aus, dass ein Personenbezug vorliegt und fragen Sie bei ihrem Vorgesetzten oder dem betrieblichen Datenschutzbeauftragten nach, wenn Sie unsicher sind, wie Sie mit den Daten umgehen sollen.
Auch Daten ohne direkten Personenbezug (z. B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen geschlossen werden kann (z. B. Personalnummer, PC-Benutzerkennung, Kfz-Kennzeichen).

Der Umgang mit personenbezogenen Daten ist nur beschränkt zulässig:
Der Umgang mit personenbezogenen Daten ist nur zulässig, wenn die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

- Personenbezogene Daten müssen auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).
- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung**

durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

- Personenbezogene Daten dürfen grundsätzlich nur für die Zwecke (weiter) verarbeitet werden, für die sie erhoben bzw. erstmals gespeichert worden sind, z.B. im Rahmen eines **Vertrages**. Voraussetzung ist allerdings, dass die **betroffene Person über die Zwecke hinreichend informiert wurde**.
- Nur in **gesetzlich bestimmten Fällen** oder mit **Einwilligung** der betroffenen Person ist eine anderweitige Verarbeitung zulässig (z.B. die Weitergabe an Dritte).
- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es der festgelegte Zweck erfordert. Unrichtige oder unvollständige Daten sind zu löschen oder zu berichtigen.
- Ausnahmsweise ist eine Verarbeitung auch aufgrund eines **berechtigten Interesses** zulässig, wenn keine Interessen der betroffenen Person dagegen stehen und überwiegen. Die hierbei notwendige Abwägung erfordert i.d.R. aber die Einschaltung des Datenschutzbeauftragten.
- Die Übermittlung in Länder außerhalb der EU/EWR-Staaten ist nur bei bestimmten Ausnahmen zulässig.

Technische und organisatorische Sicherheitsmaßnahmen

Es ist gesetzlich vorgeschrieben, dass personenbezogene Daten durch bestimmte technische und organisatorische Maßnahmen geschützt werden müssen. Obwohl wir die notwendigen Maßnahmen grundsätzlich organisiert haben, sind Sie als **Mitarbeiter für die Umsetzung mitverantwortlich**. Richtiges Verhalten gemäß Arbeitsvertrag und Arbeits-/Dienstanweisung ist unabdingbar. Im Folgenden einige ausgewählte Beispiele:

Zugriff bzw. der Einblick 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** (z.B. Passwort) und den entsprechenden Systemen (z.B. Sperre des PC bei Abwesenheit vom Arbeitsplatz/Büro).

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 **mitverantwortlich, um Gefährdungen zu verhindern**. Beispiele sind die Weitergabe von USB-Sticks, CD-ROM oder sonstigen externen Speichermedien sowie Daten per E-Mail, wobei i.d.R. eine passwortgeschützte Verschlüsselung der Daten erforderlich ist.

Rechte der betroffenen Person (Auswahl):

Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber der speichernden Stelle grundsätzlich das Recht auf **Auskunft** über gespeicherte Daten, Zweck und Rechtsgrundlage der Speicherung sowie Herkunft und Empfänger von Übermittlungen. Unzutreffende Daten sind zu **berichtigen**, unzulässig gespeicherte oder nicht mehr erforderliche Daten zu **löschen**.

Wenn jemandem durch eine unrechtmäßige automatisierte Verarbeitung seiner personenbezogenen Daten ein materieller oder immaterieller Schaden zugefügt wird, kann diese Person **Schadenersatz** verlangen. Weitere Rechte der betroffenen Personen sind aus Gründen der Übersichtlichkeit hier nicht weiter aufgeführt.

Wichtig ist in jedem Fall, dass bei entsprechenden Anfragen der betroffenen Personen eine zeitnahe Bearbeitung und Beantwortung gewährleistet wird. Jeder Mitarbeiter ist daher verpflichtet, ihm bekannt werdende Anfragen oder Anträge im Zusammenhang mit dem Datenschutz unverzüglich zur Bearbeitung aufzugreifen bzw. nach Absprache weiterzuleiten.

Jedermann hat das Recht, sich unmittelbar an den betrieblichen Datenschutzbeauftragten oder auch direkt an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt zu sein.

Arbeitsrechtliche Verantwortlichkeit

Neben der in der Verpflichtungserklärung aufgeführten Strafbarkeit von Verstößen gegen die Datenschutzvorschriften stellt die Missachtung von Sorgfaltspflichten beim Umgang mit personenbezogenen Daten regelmäßig eine Verletzung von Verpflichtungen aus dem Beschäftigungsverhältnis dar. Diese Verpflichtungen und Einzelmaßnahmen ergeben sich aus Ihrem **Arbeitsvertrag, einzelnen Betriebsvereinbarungen bzw. entsprechenden Betriebsanweisungen oder Richtlinien/Policies**, mit denen sich jeder Mitarbeiter regelmäßig und eigenständig vertraut machen muss. Ein Verstoß hiergegen oder eine Missachtung kann zu arbeitsrechtlichen Konsequenzen führen.

Allgemeine Verhaltensregeln beim Umgang mit Daten:

- Nur sichere Passwörter nutzen (z.B. mit Sonderzeichen/Ziffern, keine Namen) und unbedingt vertraulich halten (auch gegenüber Kollegen, Vorgesetzten oder EDV-Mitarbeitern).
- Sichern Sie die Ihnen anvertrauten Daten und Datenträger, Akten und Schriftstücke mit personenbezogenen Daten oder sonstigem vertraulichen Inhalt vor dem Zugriff Unbefugter durch Verschließen; das gilt insbesondere bei längerer Abwesenheit vom Arbeitsplatz/Büro und zum Feierabend.
- Bildschirme und PC sind bei Verlassen des Arbeitsplatzes/Büros zu sperren.
- Laptops sind bei Reisen sorgfältig zu sichern, besonders im Auto, Hotel oder auf Flughäfen.
- Keine vertraulichen Informationen per Fax schicken; falls doch erforderlich, sind besondere Vorkehrungen zu treffen; z.B. telefonische Absprache wegen Anwesenheit des Empfängers, Doppelkontrolle der Richtigkeit der gewählten bzw. eingegebenen Fax-Nummer vor Versand.
- Bevor Sie eine E-Mail mit vertraulichem Inhalt versenden bzw. beantworten, ist die Liste der möglichen Empfänger zu überprüfen! (Achtung: vertrauliche Informationen über E-Mail außerhalb unseres Netzwerkes grundsätzlich nur dann versenden, wenn eine Verschlüsselung (z.B. mit Passwort) genutzt werden kann.)
- Die Nutzung von „offenen" E-Mail-Verteilern ist zu unterlassen, wenn darin externe Empfänger enthalten sind. Ausnahme: Es gibt gute Gründe, dass alle Empfänger im „offenen" Verteiler voneinander wissen dürfen oder müssen, an wen diese E-Mail sonst noch geschickt wurde. Verstecken lässt sich der Adressverteiler, wenn die E-Mailadressen oder die Verteiler-Gruppe ausschließlich in das „BCC-Feld" (statt in das „AN-" oder „CC-Feld") eingetragen werden.
- Vernichten Sie nicht mehr benötigte Datenträger (Papier und elektronische) datenschutzkonform, so dass eine missbräuchliche Verwendung der Daten nicht mehr möglich ist.
- Wenn Ihnen eine Datenpanne bekannt wird (d.h. dass personenbezogene Daten fehlerhaft an Dritte übermittelt wurden oder auf andere Weise Unbefugten verfügbar geworden oder zur Kenntnis gelangt sind), informieren Sie unverzüglich Ihren Vorgesetzten und/oder den Datenschutzbeauftragten.
- Keine vertraulichen Gespräche/Telefonate in der Öffentlichkeit führen, wenn unbeteiligte Dritte den Inhalt mithören können.

Datenschutz geht uns alle an, denn das Vertrauen unserer Mitarbeiter, Kunden und Geschäftspartner ist nicht zuletzt von einem gesetzeskonformen Verhalten unseres Hauses abhängig.

Im Übrigen appellieren wir an Sie:

Behandeln Sie die Daten anderer so,
wie Sie Ihre eigenen Daten behandelt wissen möchten!