VERPFLICHTUNGSERKLÄRUNG DATENGEHEIMNIS UND SCHWEIGEPFLICHT

Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Allgemeine gesetzliche Anforderungen

- Es ist untersagt, personenbezogene Daten und/oder vertrauliche Unternehmensdaten unbefugt zu verarbeiten, anderen Personen mitzuteilen oder zugänglich zu machen.
- Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei der Tätigkeit als mitwirkende Person gemäß § 203 StGB (Privatgeheimnis) bekannt geworden ist.
- Die Pflicht zur Wahrung des Datenschutzes und der Verschwiegenheit bleibt auch im Falle einer Versetzung oder nach Beendigung des Arbeitsverhältnisses bestehen.
- Auch in einer häuslichen Arbeitsstätte ist der Schutz von Daten und Informationen gegenüber Dritten einschließlich Familienangehörigen zu gewährleisten. Vertrauliche Daten und Informationen sind so zu schützen, dass Dritte sie nicht einsehen und nicht auf sie zugreifen können.
- Für Mitarbeiter/innen der Informations- und Kommunikationstechnik gilt zusätzlich: Das Fernmeldegeheimnisses ist zu wahren. Demnach ist es mir untersagt, mir oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

Ich verpflichte mich zur Einhaltung der oben genannten Vorgaben und:

- das Gesetz über den kirchlichen Datenschutz – KDG – sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen/Gesetze/Obliegenheiten (Verhaltenspflichten) einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in der jeweils geltenden Fassung sorgfältig einzuhalten.
- das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten. Ich bin darüber belehrt worden, dass ein Verstoß gegen geltende Datenschutzvorschriften disziplinarrechtliche beziehungsweise arbeitsrechtliche und auch strafrechtliche Folgen (Verletzung von Privatgeheimnissen gemäß § 203 StGB) haben kann.
- Beispiele für einen Verstoß gegen die Vorgaben des Datenschutzes wären: 1) Einsichtnahme in eine Patienten- /Bewohnerakte für der/die Mitarbeiter/in keine Aufgabenerfüllung hat; 2) Weitergabe von Informationen über Patienten/Bewohner im außerdienstlichen Umfeld; 3) Fotografieren und/oder weiterleiten von Patienten/Bewohnerbildern, Röntgenbilder, Wundaufnahmen insbesondere an Soziale Netze.

Ich bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Datenschutzbestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass das KDG und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften persönlich zu den üblichen Geschäftszeiten in der Personalabteilung sowie elektronisch im Dokumentenlenkungssystem (Nexus Curator) eingesehen werden können.

Die **Anlage** zu dieser Verpflichtungserklärung enthält wichtige Hinweise und Empfehlungen zur Einhaltung des Datenschutzes. Diese werde ich lesen und beachten.

Diese Erklärung wird Bestandteil meiner Personalakte.

Anlage
Hinweise und Empfehlungen zum Datenschutz

Der für Sie zuständige verantwortliche Datenschutzbeauftragte ist:	**Herr Josef Schwarzkopf**
Kontaktdaten: Tel. 0 23 82/858 – 118	**E-Mail: josef.schwarzkopf@sfh-ahlen.de**

DATENSCHUTZ AUF PC UND SERVER-LAUFWERK

- Es müssen sichere Passwörter ausgewählt werden (8 Stellen, Groß- und Kleinbuchstaben, Zahlen, keine Namen).
- Passwörter dürfen nicht an Dritte weitergeben gegeben werden
- Nur der autorisierte Mitarbeiter darf mit der persönlichen Kennung am PC arbeiten.
- Bildschirme und PCs sind bei Abwesenheit vom Arbeitsplatz zu sperren (auch bei nur kurzzeitiger Abwesenheit)
- Der Zugriff auf das Firmennetz erfolgt ausschließlich über die VPN-Verbindung.
- Die Nutzung firmeneigener Hard- und Software ist für Dritte untersagt.
- Werden Gesundheitsdaten auf mobilen Geräten und Datenträgern gespeichert werden, sind diese Daten verschlüsselt abzuspeichern. Das Verschlüsselungsverfahren ist dem Stand der Technik angemessen auszuwählen.

FAX

- Die externe Informationsweitergabe per Fax ist grundsätzlich zu hinterfragen. Es ist vorab immer zu prüfen, ob ein Versand von sensiblen Daten mit der Post zeitlich möglich und sicherer ist. Ist dies nicht möglich, ist ein vorheriges Telefonat mit dem Empfänger zu führen und eine sofortige Entnahme zu vereinbaren.

E-MAIL VERKEHR

- Die Weiterleitung von dienstlichen Postfächern auf private Accounts ist untersagt.
- Antwortfunktion kann Falsche erreichen, Virengefahr bei Anlagen!

TELEFON / MOBILTELEFON

- Bei Mobiltelefonen die PIN-Nummer zur Geräteentsperrung einschalten.
- Bei sensiblen, beruflichen Gesprächen hört kein Dritter mit.
- Patientenbezogene Informationen dürfen grundsätzlich nicht per Telefon an Unbefugte weitergegeben werden.

BÜRO UND SCHREIBTISCH

- Vertrauliche und sensible Unterlagen verschließen.
- Vertrauliches nur persönlich abgeben.
- PC-Bildschirme sind so zu platzieren, dass Unbefugte keinen Einblick haben (nicht zu Fenstern und Türen).
- Es ist sicherzustellen, dass bei Tätigkeiten im Homeoffice kein Dritter (z.B. Familienmitglieder) Einblick auf firmeninterne Daten hat.
- Wenn ein Besucher ein Büro betritt, in dem vertrauliche Daten verarbeitet werden und der Mitarbeiter das Zimmer zur Bearbeitung einer Anfrage oder aus anderen Gründen verlassen muss, hat auch der Besucher bis zur Rückkehr des Mitarbeiters das Zimmer zu verlassen.
- Büros müssen nach jedem Verlassen abgeschlossen bzw. bei Vorhandensein eines starren Knaufs zugezogen werden. Schränke, in denen personenbezogene Mitarbeiterdaten gelagert werden, müssen abgeschlossen werden.

DATENMÜLLENTSORGUNG

- Schredder oder Datenmülltonne verwenden.
- Datenträger (CD, Festplatten, etc.) sind fachgerecht nur über das Datenmüll-Entsorgungsunternehmen bzw. FACT IT zu entsorgen.

Im Zweifel gilt: Sprechen Sie den für Sie zuständigen Datenschutzbeauftragen an. Dieser berät Sie gerne.