Informationsblatt Datenschutz

Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse hat. Ein schutzwürdiges Interesse ist grundsätzlich anzunehmen – außer bei Daten aus allgemein zugänglichen Quellen (z. B. Telefonbuch).

Daher ist jedermann verpflichtet, personenbezogene Daten Dritter geheim zu halten.

Unter personenbezogenen Daten versteht man gemäß der EU-Datenschutzgrundverordnung (DS-GVO) Angaben über natürliche Personen z. B. Name, Adresse, Geburtsdatum, Beruf, Versicherungsdaten, Bankverbindung, Kfz-Kennzeichen, Einkommensverhältnisse, Interessen etc.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten unterliegt einem besonderen Schutz. Dabei handelt es sich um Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben oder sexuelle Orientierung sowie genetische und biometrische Daten.

Das bedeutet, dass Daten von Patienten grundsätzlich zu den besonders geschützten Daten gehören, deren Verarbeitung zusätzlichen Einschränkungen unterliegt.

Unter Verarbeiten von Daten versteht man jede Art der Handhabung von Daten, also das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen (durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung), Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten von Daten.

Das Datengeheimnis bedeutet, dass Daten, die Ihnen im Rahmen Ihrer Tätigkeit anvertraut oder bekannt werden, von Ihnen geheim zu halten sind. Sie dürfen diese Daten nur dann an Dritte weitergeben, wenn Ihnen dies ausdrücklich angeordnet wird. Das schließt auch die Einhaltung von Sicherheitsmaßnahmen ein, damit Daten Unbefugten nicht zur Kenntnis gelangen oder von diesen eingesehen werden können.

Generelle Sicherheitsvorschriften

- Die Hardware, die Software und der Zugang zum KAGes-Netz werden Ihnen zur Erfüllung der Ihnen übertragen Aufgaben zur Verfügung gestellt. **Modifikationen an der Hardware oder Installieren weiterer Software sind nicht erlaubt.**

- Benützen Sie dienstliche Daten nur zur Erfüllung Ihrer Aufgaben. **Jede Weitergabe – auch an Kollegen – ohne dienstliche Notwendigkeit ist verboten.**

- Ihr persönliches Passwort ist der Zugangsschlüssel, der die Datenanwendung vor dem Zugang unautorisierter Personen schützt. Zugleich übernehmen Sie durch die Eingabe Ihres Passwortes – wie mit einer Unterschrift – die Verantwortung für das, was Sie innerhalb

der Datenanwendung tun. **Die Weitergabe des Passwortes ist daher auch in Ihrem Interesse streng verboten.**

- **Auch Zugangsdaten zu Datenanwendungen außerhalb der KAGes sind geheim zu halten.** Wenn Sie beispielsweise Web-Applikationen nutzen, um auf Befunde Ihrer Patienten, die z. B. von niedergelassenen Radiologen erstellt wurden, zuzugreifen, dürfen Sie diesen Benutzernamen und das dazugehörige Passwort nicht an öffentlich zugänglichen Stellen (z. B. Pinwand) notieren.

- **Ihre Aktivitäten** in den IT-Systemen **werden mitprotokolliert und können daher Ihrer Person zugeordnet werden.**

- **Melden Sie sich vom System ab, wenn Sie es nicht mehr benötigen. Bei kurzzeitigen Abwesenheiten sperren Sie den Bildschirm.**

- **Ausdrucke mit Patienten-, Mitarbeiter- oder Firmendaten dürfen Unbefugten nicht zugänglich gemacht werden.** Verwahren Sie sie deshalb sorgfältig. Wenn Sie sie nicht mehr benötigen, entsorgen Sie sie so, wie es in Ihrem Bereich vorgesehen ist (z. B. Reißwölfe oder entsprechend gekennzeichnete Sammelbehälter).

- **Sie dürfen Daten nicht außerhalb der KAGes verbringen**, auf welchem Medium auch immer (Papier, Datenträger, Notebook, Handy, Kamera etc.) – ausgenommen, wenn Sie das im dienstlichen Auftrag zu dienstlichen Zwecken tun.

- Wenn Sie dienstliche Daten in Ihrem Handy (z. B. im Kalender) notieren, **achten Sie darauf, keine personenbezogenen Daten preiszugeben** (z. B. „10:00 Hüft-Operation“ aber ohne den Namen des Patienten!). Diese Daten werden üblicherweise automatisch gesichert, d. h. auf Server bei z. B. Apple oder Google übertragen und eventuell auch auf Ihren privaten Rechner zuhause gespiegelt, zu dem womöglich andere Personen Zugang haben.

- **Melden Sie Datenschutzverletzungen Ihrem Vorgesetzten** (oder im Falle eines Praktikums Ihrem Lehrbeauftragten oder der für Sie zuständigen Betreuungsperson) **oder dem Datenschutzbeauftragten** (Kontakt: E-Mail: datenschutz@kages.at, Tel: 0316/340-5115).