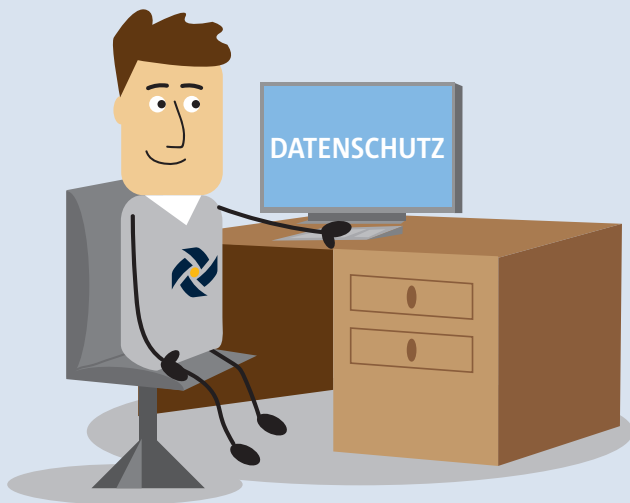


10 TIPPS ZUM DATENSCHUTZ

IN DEN MÜHLENKREISKLINIKEN



Liebe Kolleginnen und Kollegen,

die vorrangige Aufgabe des Bereichs Datenschutz ist es, die Einhaltung der Datenschutzgrundverordnung (DS-GVO), des Bundesdatenschutzgesetzes, des Landesdatenschutzgesetzes und anderer Datenschutzvorschriften in den Mühlenkreiskliniken, den zugehörigen Krankenhäusern und Verbundunternehmen zu unterstützen und zu überwachen.

Alle Beschäftigten können sich in Angelegenheiten des Datenschutzes jederzeit ohne Einhaltung des Dienstweges an den Datenschutzbeauftragten wenden. Dazu existieren verschiedene Wege zur Kontaktaufnahme, die Sie in diesem Heft finden.

Dieses Heft dient als kleine Hilfestellung zum komplexen Thema Datenschutz und zeigt mit zehn einfach dargestellten Tipps, wie die Sicherheit der Daten für alle Mitarbeiterinnen und Mitarbeiter im Arbeitsalltag verbessert werden kann.

Bernhard Bues

Datenschutzbeauftragter

Stefanie Bauer

Abteilungsleiterin Informationssicherheitsmanagement und
Datenschutz

CLEAN DESK



Eine **offene Patientenakte auf dem Schreibtisch, ein vergessener Vertrag oder ein anderes sensibles Dokument** im Kopierer können fatale datenschutzrechtliche Folgen für Patient*innen oder Mitarbeitende haben. Lassen Sie bitte keine Unterlagen mit sensiblen oder personenbezogenen Daten offen und einsehbar liegen – nicht am Drucker, Kopierer oder am Arbeitsplatz.

VERNICHTUNG ODER ABLAGE P.



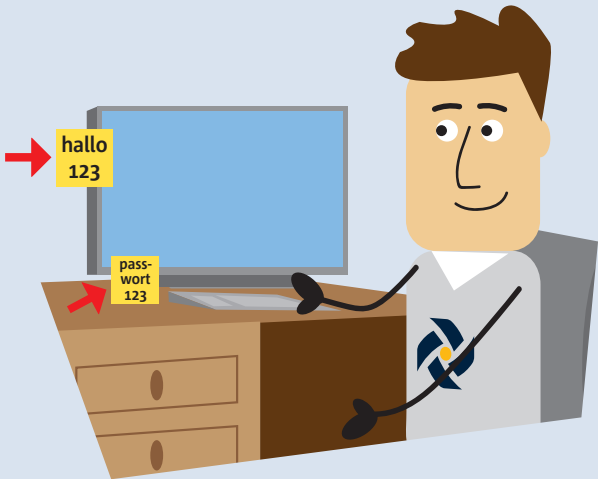
Speicherbegrenzung ist einer der Grundsätze des Datenschutzes. Daten sollten hiernach nur solange gespeichert werden, wie dies für den Zweck der Verarbeitung erforderlich ist. Nutzen Sie zur **Vernichtung sensibler oder personenbezogener Daten** auf Papier bitte nicht den Papierkorb, sondern die bereitstehenden Datentonnen oder alternativ einen Schredder.

WINDOWS-TASTE + L



Achten Sie auch bei kurzfristigem Verlassen des Arbeitsplatzes darauf, **Ihren Rechner zu sperren**. Der Tastaturbefehl hierfür ist die Tastenkombination „Windows-Taste + L“. So kann kein Unbefugter in Ihrer Abwesenheit auf Ihre Daten zugreifen.

DAS RICHTIGE PASSWORT



Account-Sharing oder das Verwenden einfacher Passwörter ist ein No-go! **Benutzerzugänge müssen durch sichere Passwörter geschützt werden.** Verwenden Sie mindestens acht Zeichen unter Kombination von Klein- und Großbuchstaben, Ziffern, Satz- und Sonderzeichen. Hilfreich beim Merken sind Eselsbrücken wie die Anfangsbuchstaben eines Satzes: „Seit dem Jahr 2021 ist mein Passwort sicher! – SdJ2021imPs!. Schreiben Sie das Passwort nicht auf und teilen Sie das Passwort mit niemandem.

AUSKUNFT AM TELEFON



Gegenüber unbefugten Dritten dürfen keine **Auskünfte zu personenbezogenen Daten gegeben werden**. Zur Vermeidung ist es unerlässlich, frühzeitig gründlich zu sensibilisieren, welche Auskünfte welcher Person gegenüber erteilt werden dürfen. Anfragen von berechtigten Angehörigen zum Gesundheitszustand von Patient*innen können nach den allgemeinen Regeln beantwortet werden. Geben Sie niemals Berufsgeheimnisse, Geschäftsgeheimnisse oder Patientendaten ohne Befugnis preis.

VORSICHT FALLE!



Die Nutzung von E-Mails gehört zum beruflichen Alltag. Bedauerlicherweise versuchen **Hacker die Schwachpunkte des E-Mail-Verkehrs nutzbar zu machen**. Bei unbekanntem E-Mails aus nicht vertrauenswürdigen Quellen, die zum Beispiel nach Log-in-Daten fragen oder Anhängen aus unbekanntem Quellen haben, ist daher Vorsicht geboten. Es könnten sogenannte Phishing-Versuche sein oder es sind Viren oder Trojaner enthalten. Sollten Sie unsicher sein, leiten Sie die betreffende E-Mail bitte an den Bereich Datenschutz (datenschutz@muehlenkreiskliniken.de) oder ISM (ism@muehlenkreiskliniken.de) weiter.

HAPPY BIRTHDAY!



Veröffentlichen Sie ohne Einwilligung keine Fotos von Mitarbeitenden oder Patient*innen in sozialen Netzwerken, im Intranet oder auf der Klinik-Website und hängen Sie keine Geburtstagslisten in Ihren Abteilungen aus. Bei Fragen wenden Sie sich bitte per E-Mail an pressestelle@muehlenkreiskliniken.de an die Abteilung für Unternehmenskommunikation und Marketing.

HEREIN!



Büroräume bieten zahlreiche Gefahren für Datenschutzverstöße, insbesondere wenn sich dort unbefugte Personen aufhalten können. Ein offenes Büro, ein unverschlossener Serverraum oder ein unbeaufsichtigtes Behandlungszimmer können fatale Folgen für den Datenschutz von Patient*innen und Mitarbeitenden haben. Der Zugang zu diesen Räumen sollte für Betriebsfremde nur für Betriebszwecke und auch nur unter Aufsicht gestattet sein.

AUS FEHLERN LERNEN



Menschen machen Fehler. Um Ärger aus dem Weg zu gehen, neigen sie manchmal dazu, Datenpannen zu verschweigen. Aus Fehlern lernt eine Organisation. Daher bitten wir Sie, alle Datenpannen zunächst an den Bereich Datenschutz (datenschutz@muehlenkreiskliniken.de) und an Ihre*n Vorgesetzte*n zu melden.

„BETROFFENEN-RECHTE“



Erhalten Sie Auskunftersuchen von Patient*innen, Angehörigen oder Behörden mit der Bitte um Mitteilung, welche personenbezogenen Daten die Mühlenkreiskliniken verarbeiten, mit der Bitte um Löschung oder Sperrung von personenbezogenen Daten, mit Widerrufern oder Widersprüchen gegen die Verarbeitung personenbezogener Daten, so leiten Sie diese Anfragen bitte sofort auch an den Bereich Datenschutz (datenschutz@muehlenkreiskliniken.de) im Hause weiter.

INFOS UND KONTAKTAUFNAHME

INFORMATIONSSICHERHEITSMANAGEMENT UND DATENSCHUTZ

Informationen

Intranet Zentrale Dienste → Informationssicherheitsmanagement und Datenschutz (ISM/DS)

Kontakt

datenschutz@muehlenkreiskliniken.de
ism@muehlenkreiskliniken.de

Telefon

0571/790-2701

DATENSCHUTZBEAUFTRAGTER

Informationen

Intranet: Zentrale Dienste → Datenschutzbeauftragter (DSB)

Kontakt

datenschutzbeauftragter@muehlenkreiskliniken.de

Telefon

0571/790-2700

Informationssicherheitsmanagement und Datenschutz

Mühlenkreiskliniken AÖR
Hans-Nolte-Straße 1
32429 Minden
datenschutz@muehlenkreiskliniken.de oder
ism@muehlenkreiskliniken.de

www.muehlenkreisklinken.de

