

Rödl & Partner

DATENSCHUTZ BEI HOME OFFICE TÄTIGKEITEN

WERTVOLLE HANDLUNGSEMPFEHLUNGEN FÜR
DIE UNTERNEHMEN DER GESUNDHEITS- UND
SOZIALWIRTSCHAFT



DATENSCHUTZ BEI HOME OFFICE TÄTIGKEITEN

In einer Phase wie der Corona-Pandemie kann unvermittelt die Notwendigkeit entstehen, Mitarbeiter im Home Office tätig werden zu lassen. Dabei sollten einige Sicherheitsregeln unbedingt beachtet werden. Dies gilt im Besonderen für Krankenhäuser, Sozialunternehmen und Pflegeeinrichtungen, deren Verwaltungskräfte teilweise ebenfalls auf das Home Office ausweichen wollen und müssen.

Die nachfolgenden Handlungsempfehlungen helfen, bei diesem Übergang Notwendigkeiten zu bedenken, die fast immer relevant sind. Die Aufstellung ist beispielhaft, kann jedoch nicht alle Bereiche vollständig abdecken. Die konkrete Lösung muss auf die Voraussetzungen im Unternehmen gezielt angepasst werden. Gerne unterstützen wir Sie bei der Erstellung der für Ihre Einrichtung geeigneten Richtlinien.



Regeln vorgeben:

Die Verhaltensregeln zur Einhaltung des Datenschutzes und der Informationssicherheit bei der Tätigkeit im Home Office sollten den Mitarbeitern leicht verständlich und in schriftlicher Form mitgeteilt werden.



Private Endgeräte nur unter bestimmten Voraussetzungen:



Sofern auf Grund fehlender Beschaffungsmöglichkeiten private Endgeräte eingesetzt werden sollen, ist unbedingt folgendes zu empfehlen:

Zeitlich begrenzt:

Die Nutzung privater Endgeräte für dienstliche Zwecke ist nur solange und in dem Umfang zulässig, wie keine dienstlichen Geräte zur Verfügung stehen.

Antiviren-Software:

Auf dem privaten Rechner muss eine professionelle Antivirus-Software installiert und aktuell gehalten werden.

VPN oder private Cloud:

Ein Zugriff des Arbeitnehmers auf die Systeme des Arbeitgebers sollte von einem privaten Endgerät aus ausschließlich unter Nutzung einer VPN-Verbindung oder allenfalls als Zugriff auf eine gesicherte private Cloud des Arbeitgebers erfolgen. Insbesondere in der Gesundheits- und Sozialwirtschaft sind andere Formen der technischen Ausgestaltung zu vermeiden. Speziell der Transfer betrieblicher Dateien auf den privaten Rechner des Arbeitnehmers, um diese in der dortigen Umgebung zu bearbeiten, sollte grundsätzlich ausgeschlossen sein.

Kein Windows 7 oder älter:

Windows 7 ist veraltet und wird von Microsoft nicht mehr mit Sicherheitsupdates versorgt. Es ist kein sicheres Betriebssystem und darf nicht auf einem privaten PC verwendet werden, der dienstlich genutzt werden soll.

In allen Fällen sollte für das Home Office gelten:

Bildschirm sperren:

Der Arbeitnehmer stellt sicher, dass Haushaltsangehörige oder Besucher keinen Zugang zu vertraulichen Daten haben. Der Benutzeraccount auf dem privaten Rechner muss daher passwortgeschützt sein. Der Bildschirm muss beim Verlassen immer gesperrt werden (Windows-Taste und Buchstabe „L“ drücken).

Clean Desk:

Aus demselben Grund dürfen keine Unterlagen in Papierform offen und zur Einsichtnahme herumliegen. Papierabfall der dienstlichen Tätigkeit muss sicher verwahrt werden und später bei der nächsten Anwesenheit im Büro datenschutzgerecht vernichtet werden, er darf nicht in den Hausmüll oder den Altpapiermüll gelangen. Während der Mitarbeiter dienstlich arbeitet, sollten keine anderen Personen anwesend sein, die Einblick in den Bildschirm nehmen oder Telefonate mithören könnten. Für den Bildschirm ist ggf. eine Sichtschutzfolie nützlich.

Sorgfältiger Umgang mit Datenträgern und Ausdrucken:

Dienstliche Hardware mit Speicherfunktionen (Rechner, Handy, Speichermedien) sowie dienstliche Unterlagen, ggf. auch im Home Office erstellte Ausdrücke dienstlicher Dokumente, müssen sorgsam verwahrt werden. Nach Arbeitsende sollten sie in einem verschlossenen Behälter gelagert werden.

Alexa muss draußen bleiben:

Intelligente Sprachausgabegeräte, wie beispielsweise Alexa, Siri etc., haben in Hörweite des Home-Office-Arbeitsplatzes nichts verloren. Dies gilt für Mitarbeiter im Gesundheitswesen in besonderer Weise. Die Abhörgefahren sind schlicht zu groß.

Datenpannen sind zu melden:

Ein meldepflichtiger Datenschutzverstoß im Sinne von Art. 33 DSGVO kann auch im Home Office erfolgen, beispielsweise wenn vertrauliche Unterlagen auf dem Tisch ausgebreitet waren und Gäste ins Haus kommen, die die darin enthaltenen personenbezogenen Daten einsehen. Arbeitnehmer müssen beim Wechsel ins Home Office dafür sensibilisiert werden, so dass ggf. eine Meldung erfolgen kann.



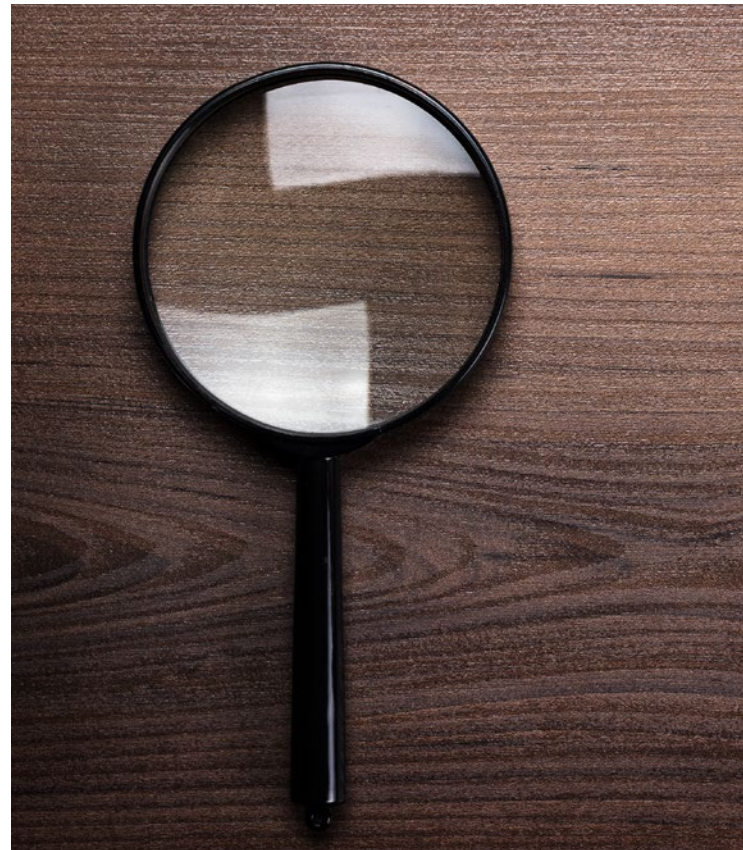
Der Arbeitgeber sollte als datenschutzrechtlich Verantwortlicher außerdem auf folgendes achten:

Besondere Vorsichtsmaßnahmen bei Gesundheitsdaten:

In Krankenhäusern und Sozialunternehmen verarbeiten die Mitarbeiterinnen und Mitarbeiter der Verwaltung regelmäßig Gesundheitsdaten der Patienten bzw. Klienten. Da diese Daten im Sinne des Art. 9 DS-GVO als besonders schutzbedürftig gelten, sind gerade auch für Home-Office-Phasen besondere Schutzvorkehrungen notwendig. Diese sollten mit dem Datenschutzbeauftragten entwickelt und in der Aufstellung der technischen und organisatorischen Maßnahmen dokumentiert sein.

Erforderlichkeit einer Datenschutzfolgenabschätzung prüfen und dokumentieren:

Die Verarbeitung von Patientendaten, z.B. im Abrechnungssystem eines Klinikums, die im Home Office erfolgt, könnte auf Grund der Umstände der Verarbeitung (häusliches Umfeld des Klinikmitarbeiters) als besonders risikoträchtig angesehen werden. In diesem Fall ist eine Datenschutzfolgenabschätzung nach Art. 35 DS-GVO erforderlich.



IHRE ANSPRECHPARTNER



Christoph Naucke

Betriebswirt (Berufsakademie), Zertifizierter Compliance Officer,
Zertifizierter Datenschutzbeauftragter

T +49 911 9193 3628
E christoph.naucke@roedl.com



Jürgen Schwestka

Diplom-Kaufmann, CISA, Zertifizierter IT-Security-Auditor,
IT-Auditor^{IDW}, Leiter Assurance & IT

T +49 911 9193 3508
E juergen.schwestka@roedl.com

Gerne stehen wir für weitergehende Fragen zur Verfügung!

MEHR INFOS GEFÄLLIG?

*Informative Whitepaper
hilfreiche Checklisten
und viele Flyer*

zu den verschiedensten Themen der
Gesundheits- und Sozialwirtschaft



Jetzt kostenfrei herunterladen: www.roedl.de/downloadcenter-gesundheit-sozialwirtschaft

*Kennen Sie schon unsere
fachspezifischen Newsletter?*

Der E-Mail Newsticker
Kompass Gesundheit und
Soziales und der Newsletter
Fokus Gesundheits- und
Sozialwirtschaft.

Jetzt kostenfrei abonnieren:
<http://www.roedl.de/medien/publikationen/newsletter/>

