Datenschutz

Sicher arbeiten im Homeoffice

Mobiles Arbeiten und Homeoffice sind nicht mehr die Ausnahme, sondern Alltag. Es wird nicht nur von zu Hause aus gearbeitet, sondern Meetings werden via Video abgehalten, Teamabsprachen erfolgen via Chatfunktion, und Dokumente werden via Kollaborationsplattformen geteilt. Bei diesem digitalen Büroalltag in den eigenen vier Wänden dürfen der Datenschutz und die Geheimhaltung nicht vergessen gehen.

Von Dr. Stefan Rieder

Das ortsungebundene Arbeiten – also sowohl Homeoffice als auch mobiles Arbeiten – ist aus dem Unternehmensalltag nicht mehr wegzudenken. Arbeitnehmende arbeiten derzeit nicht nur von zu Hause aus, sondern besuchen teilweise ihre Familie im In- oder Ausland und arbeiten dort vor Ort digital. In Bezug auf das mobile Arbeiten sollte man sich als Unternehmen die Frage stellen, ob das Arbeiten ausserhalb der Räumlichkeiten des Unternehmens generell (Homeoffice, Coworking Spaces oder an einem beliebigen Ort) oder nur im Homeoffice des Mitarbeitenden zugelassen werden soll. Beim mobilen Arbeiten darf nicht ausser Acht gelassen werden, dass unter Umständen ein erhöhtes Sicherheitsrisiko besteht, das Cyberkriminelle versuchen auszunutzen. Das gilt umso mehr, wenn das Homeoffice als neuer Büroalltag sehr abrupt eingeführt worden ist.

Datenschutz

Der Datenschutz im Homeoffice geht oftmals vergessen oder wird unzureichend umgesetzt. Die Verantwortung des Unternehmens zur Gewährleistung des Datenschutzes bleibt uneingeschränkt bestehen, auch für mobiles Arbeiten im Homeoffice oder anderswo. Auch im Homeoffice oder an jedem beliebigen mobilen Arbeitsort muss der Datenschutz angemessen mit geeigneten technischen und organisatorischen Massnahmen durch das Unternehmen gewährleistet werden. Hierzu gehört zum Beispiel das Vorsehen eines sicheren Datentransfers vom und in das Homeoffice etwa durch verschlüsselte Verbindungen oder durch webbasierte Oberflächen, bei denen nicht

Passwörter für Video-Meetings sollten nicht zusammen mit der Einladung, sondern in einer separaten E-Mail mitgeteilt werden.

nur die Daten, sondern auch die Anwendungen zentral auf dem Unternehmensserver bleiben. Ebenfalls unerlässlich ist, dass das Betriebssystem und die verwendeten Programme immer mit den zur Verfügung stehenden Updates aktualisiert sind, um Sicherheitslücken zu schliessen.

Weiter ist es wichtig, dass die Vertraulichkeit der Daten sowie der geschäftlichen Dokumente jederzeit sichergestellt ist und der Zugriff darauf nur durch den jeweiligen Arbeitnehmenden möglich ist und nicht durch unberechtigte Personen wie Familienmitglieder, Freunde oder sonstige Besucher. Es sollte eine Selbstverständlichkeit sein, dass die im Homeoffice genutzte Hardware passwortgeschützt ist und der Sperrschutz beim Verlassen des Arbeitsplatzes aktiviert wird. Anderen Bewohnern ist die Nutzung des Endgerätes, sofern es sich nicht um ein eigenes Gerät des Arbeitnehmenden handelt (Bring Your Own Device), zu untersagen.

Die Arbeit im Homeoffice findet zudem idealerweise in einem separaten, abschliessbaren Raum (Büro zu Hause) und nicht am Esstisch statt. Gerade zu Hause empfiehlt es sich, eine klare Clean-Desk-Policy vorzugeben, damit alle Dokumente – sofern im Homeoffice nicht papierlos gearbeitet wird – am Ende des Arbeitstages vor dem Zugriff durch andere Personen geschützt sind. Idealerweise sollte auf Ausdrucke geschäftlicher Dokumente im Homeoffice verzichtet werden, sofern diese online verfügbar sind. Falls geschäftliche Dokumente physisch im Homeoffice vorhanden sind, ist nach ihrem Verwendungszweck sicherzustellen, dass sie nicht zusammen mit dem Hausmüll entsorgt werden.

Musterklausel Geheimhaltung

1. Der Arbeitnehmer ist verpflichtet, geschäftliche Unterlagen, die für die Erfüllung seiner Arbeiten im Homeoffice benötigt werden, geheim zu halten. Sie dürfen nicht unbeaufsichtigt liegen gelassen oder Dritten in irgendeiner Form zugänglich gemacht werden. Der Laptop ist mit einem Passwort und einer Sichtschutzfolie zu schützen.
2. Telefonate sind so zu führen, dass sie nicht durch unbefugte Dritte mitgehört werden können und keine Störungen erfolgen.
3. Die Wahrung des Geschäftsgeheimnisses ist jederzeit sicherzustellen. Im Übrigen gilt Ziff. XY des Personalreglements.

Telefon- und Videokonferenzen

Bei der Arbeit im Homeoffice erfolgt die Kommunikation nicht nur über das Telefon und Videoanrufe, sondern es werden oftmals Kommunikations- und Kollabora-

tionstools verwendet. Bei den eingesetzten Tools sollte sorgfältig geprüft werden, ob der Datenschutz gewährleistet ist. Zudem sollten bei Online-Meetings – wie auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) empfiehlt – generell einige Punkte beachtet werden:

- Meeting-IDs sollten nicht allgemein zugänglich geteilt werden, weil andernfalls unerwünschte Teilnehmer am Meeting ebenfalls teilnehmen können. Aus dem gleichen Grund sollten Meeting-IDs nur über sichere Kommunikationskanäle (z.B. verschlüsselte E-Mails) versendet werden und nicht über ein unsicheres Chatprogramm.
- Idealerweise sind einmalige Meeting-IDs zu verwenden, auch wenn ein Meeting mit dem gleichen Kreis von Teilnehmenden regelmässig stattfindet.
- Meetings sollten mit einem Passwort geschützt werden, und das Passwort ist nicht mit der Einladung, sondern mit einer separaten E-Mail mitzuteilen.
- Sowohl bei Beginn des Meetings als auch während des Meetings sollte der Kreis der Teilnehmenden überprüft werden. Der Organisator des Meetings sollte hierfür dafür sorgen, dass die Teilnehmenden jeweils ihren vollen Namen angeben und nicht irgendwelche Pseudonyme verwenden. Vorsicht ist auch geboten, wenn einzelne Teilnehmer eines Meetings nach dem Meeting etwas anderes weiterbesprechen wollen und in demselben Meeting verbleiben, weil unter Umständen unerwünschte Personen ebenfalls noch im Meeting sein können oder sich nach einem kurzen Abmelden wieder einloggen können.
- Sofern die (integrierte) Kamera des Endgerätes verwendet wird, sollte der Aufnahmebereich geprüft werden, damit die anderen Teilnehmenden keine vertraulichen Informationen sehen (z.B. angeschriebene Ordner im Hintergrund, herumliegende Dokumente etc.). Bei Nichtgebrauch sollte die Kamera idealerweise abgedeckt bzw. abgeklebt werden.
- Beim Screensharing ist darauf zu achten, dass nur die relevanten Anwendungen geöffnet sind. Nicht selten bleibt während einem Meeting das E-Mail-Programm offen, und wenn der ganze Bildschirm geteilt wird und nicht nur eine bestimmte Anwendung, dann kann zum Beispiel das Vorschaufenster eingehender E-Mails für alle Teilnehmenden ersichtlich sein.
- Sofern ein Meeting aufgenommen wird, muss das bei Beginn angekündigt werden, weil die Teilnehmenden damit einverstanden sein müssen. Ohne Einverständnis aller Teilnehmenden darf ein Meeting nicht aufgezeichnet werden, bzw. die damit nicht einverstandenen Personen müssen das Meeting verlassen können.

Datenschutzrichtlinien der Anbieter von Kommunikationstools überprüfen

Anbieter von Videokonferenzlösungen haben oftmals Zugriff auf bestimmte persönliche Daten wie zum Beispiel die Dauer des Meetings, Standortdaten, Teilnehmeridentifikationen (Vorname, Nachname, E-Mail-Adresse) und Anzahl der Teilnehmenden, und diese Daten werden unter Umständen an (ausländische) Dritte weitergegeben. Eine solche Weitergabe muss aus der Datenschutzrichtlinie des Anbieters hervorgehen, und es lohnt sich, diese Datenschutzrichtlinie im Detail zu studieren. Vor der Nutzung des Videokonferenztools lohnt es sich auch, die Datenschutzeinstellungen des Programms anzusehen und gegebenenfalls anzupassen.

SEMINARTIPP

Homeoffice und flexibles Arbeiten rechtssicher gestalten

Stolpersteine bei modernen Arbeitsformen vermeiden

- Dienstag, 30. März 2021
- Donnerstag, 25. November 2021

Seminarleiter: Dr. Stefan Rieder

Zentrum für Weiterbildung der Uni Zürich

Mehr Informationen unter www.praxisseminare.ch

Dr. Stefan Rieder ist als Fachanwalt SAV Arbeitsrecht im privaten Arbeitsrecht, öffentlichen Personalrecht und Sozialversicherungsrecht sowohl beratend als auch prozessierend tätig.