Bild: iStock.com/AleksandarNakic

Einträchtiges Arbeiten von zu Hause aus - derzeit wohl keine seltene Situation

Mit Richtlinien arbeiten

Homeoffice und Datenschutz so passt beides zusammen

Die Corona-Krise hat dafür gesorgt, dass mehr Beschäftigte im Homeoffice arbeiten als jemals zuvor. In der ersten Not war der Datenschutz oft kein Thema. Das sollte sich nun ändern.

Viele Unternehmen haben in Rekordzeit ihre Mitarbeiter ins Homeoffice geschickt. Dass dabei sicher nicht der Datenschutz im Vordergrund stand, sondern die Beschäftigten zu schützen und den Betrieb irgendwie aufrechtzuerhalten - verständlich und geschenkt. Doch nun ist es an der Zeit, näher hinzuschauen und für geregelte Bahnen auch in puncto Datenschutz zu sorgen.

„Homeoffice" ist nicht gesetzlich definiert

Ebenso wie viele andere immer wieder verwendete Begriffe - mobile office, remote work oder mobile Arbeit - ist das ,,Homeoffice " nicht (gesetzlich) definiert.

Geht es darum, die Arbeitsleistung außerhalb des vereinbarten Dienstorts zu erbringen, ist allein der Begriff„Telearbeit" eindeutig bestimmt. So legt § 2 Abs. 7 der Arbeitsstättenverordnung fest, dass Telearbeitsplätze Bildschirmarbeitsplätze sind, die der Arbeitgeber im Privatbereich des Beschäftigten fest eingerichtet hat. Bei der Telearbeit geht es also ausschließlich um die Arbeit von zu Hause mithilfe eines vom Arbeitgeber eingerichteten Arbeitsplatzes.

Daraus entstehen sowohl für den Arbeitgeber als auch für die Beschäftigten Rechte und Pflichten (Kostentragung, Zutrittsrecht, Vertraulichkeit, Gestaltung des Arbeitsplatzes etc.), die einer ausdifferenzierten Vereinbarung bedürfen . In der aktuellen Situation wünschen sich zwar sowohl Vorgesetzte wie Beschäftigte “von zu Hause aus zu arbeiten ". Keiner der Beteiligten möchte aber deshalb gleich einen Telearbeitsplatz einrichten müssen.

Mit„Homeoffice" ist nicht nur zu Hause gemeint

Vor diesem Hintergrund wird der Begriff „Homeoffice" vielfach missverständlich und zu eng verwendet. Denn trotz des Wortteils „home" heißt „Homeoffice" nicht zwingend, einen Arbeitsplatz zu Hause zu haben. Es geht vielmehr darum, generell mobil zu arbeiten. Das kann zu Hause sein, aber in den Zeiten vor und nach Corona auch im Zug, am Flughafen oder anders wo.

Dass eine gesetzliche Definition fehlt, macht es möglich, diese mobile Arbeit nach den Wünschen der Beteiligten und den technischen Möglichkeiten des Unternehmens (nahezu) frei und individuell zu gestalten. Diese Ausgestaltung sollte der Arbeitgeber schriftlich festhal- ten. Geht es nicht nur um eine vorüber- gehende Einrichtung wie derzeit vielfach, bietet sich beispielsweise ein Zusatz zum Arbeitsvertrag an.

Dabei kommt es den Beteiligten zugute, dass zu den Gebieten, die hierbei zu regeln sind (Arbeitszeit, Arbeitsschutz, Vertraulichkeit, Einbezug der Personal- bzw. Arbeitnehmervertretung etc.), und auch zum Datenschutz vielfach schon Vereinbarungen und Regeln existieren. Auf diese bestehenden Absprachen lässt sich für die Arbeit, die nicht am vereinbarten Dienstort erbracht wird, verweisen. Denn auch mobile Arbeit ist letztlich immer vertragliche Arbeitsleistung!

Richtlinie für Datenschutz und Datensicherheit

Da der Arbeitgeber als der im datenschutzrechtlichen Sinne „Verantwortliche" in der Pflicht ist, das geltende Datenschutzrecht einzuhalten, haftet er auch für etwaige Datenschutzverstöße, die in seinem Verantwortungsbereich liegen. Vereinbaren Arbeitgeber und Arbeitnehmer also das Arbeiten im Homeoffice, sollte dies in der Regel auf Grundlage

einer existierenden Richtlinie bzw. auf Basis einer entsprechenden Vereinbarung mit dem Beschäftigten erfolgen.

Diese Richtlinie bzw. Vereinbarung sollte mit Blick auf Datenschutz und Datensicherheit zumindest die folgenden Aspekte berücksichtigen:

Informationen und Equipment sicher aufbewahren

- Arbeiten die Beschäftigten nicht mit privater Ausstattung: Alle Eigentumsrechte an zur Verfügung gestellter Hardware, Software, Apps und Daten liegen beim Arbeitgeber. Er besitzt zu jeder Zeit das Recht, darauf zuzugreifen.
- Die Mitarbeiter dürfen nur genehmigte IT-Systeme, Anwendungen oder Dienste nutzen, um auf Unternehmensinformationen zuzugreifen, sie zu speichern oder zu verarbeiten.
- Unternehmensinformationen dürfen die Mitarbeiter nur auf tragbaren Geräten oder Wechseldatenträgern speichern, bei denen die Verschlüsselung aktiviert ist.

Zulässige IT-Nutzung

- Die vorinstallierten Sicherheitsfunktionen auf den IT-Systemen dürfen nicht modifiziert, entfernt oder anderweitig umgangen werden.
- Die Beschäftigten dürfen keine unternehmensfremden tragbaren Geräte an die IT-Systeme anschließen und auch keine fremden Geräte direkt mit dem Firmennetzwerk verbinden.
- Das mobile Arbeiten darf drahtlose Internetverbindungen nutzen (z.B. eigener Mobilfunk- oder Kabelanbieter oder Hotel-WLAN). Aber der Zugang zum Unternehmensnetzwerk muss in gesicherter Form erfolgen (z.B. über VPN).
- Unternehmensinformationen und tragbare Geräte, auf denen solche Informationen gespeichert sind, muss der Beschäftigte persönlich bei sich führen oder an einem sicheren Ort verschlossen aufbewahren.

Clear Desk

- Vertrauliche oder geheime Informationen dürfen niemals unbeaufsichtigt auf dem Schreibtisch liegen bleiben. Die Beschäftigten sollten Informationen sicher in einem verschlossenen Schrank aufbewahren, wenn sie nicht in Gebrauch sind.
- Tragbare Geräte, Sicherheitstoken und Schrankschlüssel müssen nach jedem Arbeitstag weggeschlossen bzw. vor dem Zugriff Dritter geschützt werden.
- Beschäftigte müssen die Bildschirmsperre auf ihrem Computer oder ihrem tragbaren Gerät aktivieren, wenn sie ihren Schreibtisch bzw. das Gerät unbeaufsichtigt lassen.
- Nur legitimierte Personen dürfen vertrauliche oder geheime Informationen auf dem Bildschirm einsehen.

Vor dem Klicken: nachdenken

- Beschäftigte müssen die Quellen von E-Mails, Nachrichten, Anrufen und Verbindungen in den sozialen Medien überprüfen, bevor sie Informationen weitergeben, auf Links klicken, Anhänge öffnen oder andere Anweisungen befolgen.
- Mitarbeitende müssen Vorsicht walten lassen, bevor sie Anhänge öffnen oder auf Links klicken, die zu Inhalten auf fremden Websites führen.

Umgang mit Passwörtern

- Passwörter, PINs oder Zugriffscodes dürfen niemals an andere weitergegeben werden.
- Beschäftigte dürfen ihre Unternehmens-Kontennamen, die E-Mail-Adresse oder die Passwörter nicht verwenden, um sich für private Zwecke in externen Diensten anzumelden.

Sicherheitsvorfall?

- Erlangen Beschäftigte Kenntnis von einer Verletzung des Datenschutzrechts oder der Datensicherheit, informieren sie umgehend ihre Vorgesetzen.

Privatgeräte im Homeoffice

Einigen sich Arbeitgeber und Beschäftigte darauf, Privatgeräte betrieblich zu nutzen, ist Vorsicht geboten. Grundsätzlich gehören Privatgeräte zur Privatsphäre der Beschäftigten , in der der Arbeitgeber nichts zu suchen hat .

Zugleich muss ein Arbeitgeber sicherstellen, dass betriebliche Daten auf den privaten Geräten seiner Kontrolle unterstehen und dass die Beschäftigten gesetzliche Sicherheitsvorgaben beachten. Hierbei sind im Wesentlichen Art. 32 Datenschutz-Grundverordnung (DSGVO) und das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) zu berücksichtigen. Ein Arbeitgeber ist verpflichtet, nachzuweisen, dass er die Beschäftigten über die zu beachtenden Sicherheitsmaßnahmen unterrichtet und sich Kontrollrechte hat einräumen lassen.

Hat ein Arbeitgeber keine Vereinbarung hierzu getroffen, dann besitzt er keine Kontrollrechte im Hinblick auf die Informationen, die auf den Privatgeräten gespeichert sind, und verstößt somit in der Regel gegen gesetzliche Vorgaben.

Kann ein Arbeitgeber zudem nicht nachweisen, dass er die Beschäftigten über mögliche Risiken belehrt und sie verpflichtet hat, sie zu vermeiden, kann er nicht nachweisen, dass er ein hinreichendes Datenschutzniveau gewährleistet .

Die passende IT-Ausstattung

Zu den weiteren Aufgaben des Arbeitgebers gehört es, eine IT-Ausstattung bereitzustellen, mit der die datenschutzgerechte Arbeit im Homeoffice möglich ist. Gibt ein Unternehmen z.B. Notebooks heraus, dann nur solche mit verschlüsselter Festplatte. Das gilt auch für die vom Arbeitgeber herausgegebenen USB-Sticks.

Ein Konzept zur Vernichtung sensibler Daten vervollständigt die Liste der Aufgaben des Arbeitgebers.