Homeoffice: Notfallmässige Einführung – künftige Herausforderungen für Unternehmen aus Datenschutzsicht

Unternehmen mussten am Anfang der Corona-Pandemie aufgrund der Notstandsmassnahmen des Bundesrats innert kürzester Frist einschneidende Änderungen der Arbeitssituation hinnehmen: Konnte der Betrieb aufrechterhalten werden, verwiesen die Arbeitgeber ihre Arbeitnehmer nach Möglichkeit ins Homeoffice. Hatte ein Unternehmen diese Arbeitsform nicht bereits in der Vergangenheit angeboten, musste es seine Organisation und seine Mitarbeitenden kurzfristig auf diese neue Arbeitsform hieven – dabei sind auch datenschutzrechtliche Anforderungen umzusetzen. Je früher, desto besser …

Von Dr. iur. Reto Fanger

Auch für die betriebliche Arbeit zu Hause gelten die Datenschutzanforderungen an Unternehmen und ihre Mitarbeitenden. Beim Erstellen, Speichern und Drucken von Dokumenten oder beim Telefonieren entstehen im Homeoffice schnell heikle Situationen. Datenschutz im Homeoffice beginnt denn auch mit allgemeinen Empfehlungen zur Wahrung der Vertraulichkeit von Personendaten und Geschäftsdokumenten auf ICT-Geräten wie Laptops, Tablets oder Smartphones durch Verwendung von sicheren Passwörtern und Bildschirmschonern sowie zur Umsetzung des Clean-Desk-Prinzips. Dies alleine reicht allerdings bei Weitem nicht aus …

Welche Geräte werden eingesetzt?

Unabhängig davon, ob Unternehmen ihren Mitarbeitenden erlauben, private mobile Endgeräte im Arbeitsbereich einzusetzen oder ob sie konzerneigene Devices für die private Nutzung freigeben – offene Fragen bleiben:

Setzt das Unternehmen strategisch auf *Bring Your Own Device (BYOD),* verwenden die Mitarbeitenden ihre eigenen Geräte, allenfalls unterstützt durch einen Mitfinanzierungsbeitrag der Organisation. Die Arbeitgeberin ist selbstverständlich verpflichtet, für die zusätzlichen Kosten aufzukommen, welche dem Arbeitnehmenden durch die Arbeit zu Hause entstehen (Art. 327 f. OR). Falls ein Arbeitnehmer nicht über die notwendige Hard- und Software verfügt, um die angeordnete Arbeit im Homeoffice durchzuführen, muss die Arbeitgeberin diese auf eigene Kosten zur Verfügung stellen.

WICHTIGER HINWEIS

Stellt ein Arbeitnehmer die notwendige Infrastruktur von sich aus zur Verfügung, so hat die Arbeitgeberin die Auslagen für den geschäftlichen Teil der Nutzung wie z.B. zusätzliche Telefonkosten zu bezahlen. Nur in Fällen, in den es im Unternehmen keinen Mitarbeiterarbeitsplatz gibt, wird die Arbeitgeberin auch noch eine Entschädigung für die Nutzung eines Zimmers in der privaten Wohnung als Arbeitszimmer leisten müssen.

Im Modell *Corporate Ownded, Personally Enabled (COPE),* bei dem Unternehmensgeräte zur privaten (Mit-) Nutzung freigegeben sind, liegt die Verantwortung für die Bereitstellung der Geräte und Dienste beim Unternehmen, weshalb es die Kontrolle über die berücksichtigten Hersteller, Modelle und Datentarife besitzt. COPE gilt sowohl als Gegensatz zum klassischen Bereitstellungsmodell der IT, bei dem ein Gerät zugewiesen wird, das stets am Arbeitsplatz bleibt, wie auch als Gegensatz zum BYOD-Modell.

… ist was dabei vorzukehren?

Sowohl BYOD als auch COPE weisen Sicherheitsrisiken sowie arbeits- und datenschutzrechtliche Fragen auf. Beide Modelle setzen das Unternehmensnetzwerk und die Unternehmensdaten privaten Inhalten und Applikationen und somit auch privat verursachten Sicherheitsproblemen wie Malware, Viren oder Trojanern aus. Der nutzbringende Einsatz von BYOD oder COPE bedingt für alle Beteiligten die Umsetzung zahlreicher einschlägiger technischer und organisatorischer Massnahmen.

Dementsprechend müssen aus Unternehmenssicht Betriebs- und Geschäftsgeheimnisse wie auch Personendaten von Kunden sowie Mitarbeitenden geschützt werden. Zu diesen umzusetzenden Massnahmen gehören neben der Genehmigungspflicht durch bezeichnete Verantwortliche unter anderem:

- die technische und logische Trennung von geschäftlichen sowie privaten Daten
- die Verwendung eines Virtual Private Networks (VPN) oder anderer gesicherter Lösungen für den Datentransfer

- die Implementierung von Firewalls, Sandboxes, Festplattenverschlüsselung
- die Einführung von strengen Passwort-Policies
- die Schaffung von Nutzungsweisungen für Mitarbeitende
- die Regelung des Zugriffs zur Geräteüberprüfung, für Fernwartung oder zur Datenlöschung per Mobile-Device-Management-(MDM-) oder Enterprise-Mobility-Management-(EMM-)Lösungen durch das Unternehmen
- die Regelung der geschäftlichen Datenablage, die nicht auf dem mobilen Endgerät, sondern auf einem lokalen Unternehmensserver oder einer Unternehmenscloud erfolgen soll
- sowie die Einführung eines Datenlöschprozesses

Im Folgenden einige Überlegungen zu organisatorischen Massnahmen wie Zugriffsregelungen und zum Datenlöschprozess:

Zugriffsregelungen auf Homeoffice-Geräte

Problembehaftet aus datenschutzrechtlicher Sicht ist nicht nur eine systematische MDM- oder EMM-basierte Kontrolle der mobilen Endgeräte, sondern bereits der blosse Zugriff auf die Geräte durch das Unternehmen im Einzelfall: Sowohl bei BYOD wie auch bei COPE können die persönlichen Daten des Arbeitnehmers, die auf dem mobilen Endgerät bearbeitet werden, nicht von der geschäftlichen Datenbearbeitung und den entsprechenden Unternehmensdaten getrennt werden.

Bei Zugriff des Arbeitgebers auf die Geschäftsdaten kann daher der gleichzeitige Zugriff auf die privaten Arbeitnehmerdaten ohne aufwendige technische und organisatorische Massnahmen nicht ausgeschlossen werden. Gleiches gilt für Dritte, beispielsweise Familienangehörige des Arbeitnehmers, die zumindest bei BYOD diese mobilen Endgeräte ebenfalls mitbenutzen, während dies im COPE-Modell durch die Unternehmen in der Regel durch entsprechende Benutzerweisungen generell ausgeschlossen sein dürfte.

Datenlöschprozess im Homeoffice

Dem Grundsatz nach ist das datenschutzrechtliche Recht auf Löschung ein absolutes Recht, das allerdings nur dann ausgeübt werden kann, wenn personenbezogene Daten für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden oder andere Anforderungen, z.B. Archivierung, diesem Recht entgegenstehen. Unternehmen müssen somit aufzeigen können, weshalb die Daten gesammelt und verarbeitet werden und was die rechtliche Grundlage hierfür ist. Falls das Recht auf Löschung ausgeübt werden kann, müssen Unternehmen in der Lage sein, die betroffenen Daten auf Anhieb zu löschen.

Werden Daten des Arbeitnehmers aber im Homeoffice erhoben und nach Beendigung der Pandemie nicht mehr benötigt, ist der Arbeitgeber gezwungen, diese Daten zu löschen. Die Begrenzung der Datenbearbeitungsdauer ist eine konkrete Anwendung des datenschutzrechtlichen Verhältnismässigkeitsprinzips. Die Prinzipien der Verhältnis- und Zweckmässigkeit verlangen, dass die Daten nicht länger als nötig bearbeitet werden. In der praktischen Umsetzung sind die Daten entweder zu löschen oder zu anonymisieren.

Wann muss der Arbeitgeber das Homeoffice regeln?

Somit ist aus datenschutzrechtlicher Sicht – abgesehen von der generellen Gewährleistung der Datensicherheit, der technischen und logischen Trennung von geschäftlichen und privaten Daten sowie spezifizierten Nutzungsweisungen für Mitarbeitende – eine umfassende Regelung des Zugriffs zur Geräteüberprüfung, für Fernwartung sowie zur Datenlöschung inklusive transparenter vorgängiger Information der Mitarbeitenden unabdingbar.

Unternehmen, die bis vor Kurzem noch kein Homeoffice eingeführt hatten und nun von der Corona-Krise überrumpelt wurden oder die trotz gängigem Homeoffice keine einschlägigen Regelungen besitzen, sei im Sinne der Corporate Governance und Compliance empfohlen, die offenen Sicherheits- und Regulierungslücken zu schliessen, nicht zuletzt auch im Hinblick auf das revidierte Datenschutzgesetz.

AUTOR

Dr. iur. Reto Fanger ist Rechtsanwalt (ADVOKATUR FANGER – Anwaltsboutique für ICT-, Daten-, Medien- und Arbeitsrecht, Luzern; www.advokatur-fanger.ch), Partner der Swiss Business Protection AG (www.swissbp.ch), Dozent an der Hochschule Luzern, Lehrbeauftragter an der Universität Luzern sowie Co-Organisator und -Tagungsleiter des Lucerne Law & IT Summit (LITS).