datenschutzpraxis.ch

Factsheet zum Datenschutz bereitgestellt von Daniel Kettiger

Datenschutz im Homeoffice

Homeoffice ist ein Zauberwort: Arbeitnehmerinnen und Arbeitnehmer arbeite zu Hause für das Unternehmen. Hinsichtlich des Datenschutzes stellt Homeoffice aber eine erhebliche Herausforderung dar. Das Factsheet zeigt auf, wie ein datenschutzkonformes Homeoffice zu gestalten ist.

I. Grundsätzliches

Einleitung

Homeoffice – etwa auch Telearbeit genannt – schafft die Möglichkeit, dass Arbeitnehmerinnen und Arbeitnehmer von zu Hause aus arbeiten können. Homeoffice bedeutet für das Unternehmen aber keineswegs "aus den Augen, aus dem Sinn"; das Unternehmen trägt auch für Angestellte im Homeoffice die volle Verantwortung. Dies gilt auch für den Datenschutz.

Das vorliegende Factsheet zeigt für private Unternehmen und NGO auf, wie ein datenschutzkonformes Homeoffice zu gestalten ist. Für öffentliche Verwaltungen und staatliche Betriebe sind zusätzliche Aspekte zu beachten (z.B. besondere Rechtsgrundlagen, Amtsgeheimnis).

Der Datenschutz betrifft Personendaten; er ist beim Homeoffice nur insoweit zu beachten, als Personendaten verarbeitet werden. Gleichermassen wie der Datenschutz können aber auch Geschäftsgeheimnisse betroffen sein.

Wenn besonders schützenswerte Personendaten bearbeitet werden (z.B. Gesundheitsdaten, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen, Rassenzugehörigkeit, gewerkschaftliche Tätigkeiten) sind die Anforderungen an den Datenschutz erhöht.

Wenn einzelne oder mehrere Mitarbeitende oder eine Gruppe von Mitarbeitenden in einem Unternehmen in den Arbeitsmodus des Homeoffice wechseln, dann erfolgt dies in einem geordneten und geführten Prozess. Wenn in persönlichen oder gesellschaftlichen Notlagen kurzfristig zum Homeoffice gewechselt wird, dann können in der Regel – zumindest vorerst – nicht alle Anforderungen des Datenschutzes erfüllt werden. Dies erfordert eine besondere Wachsamkeit aller Beteiligter, und das Unternehmen muss bestrebt sein, möglichst rasch Datenschutzkonformität herzustellen.

Anfälligkeit von Homeoffice für Datenschutzverletzungen

Beim Homeoffice verschmelzen die Arbeitswelt und die privaten Tätigkeiten – oft auch Arbeiten und Wohnen. Dies macht Homeoffice anfällig für Datenschutzverletzungen, wie die nachfolgenden Beispiele aufzeigen.

Praxisbeispiel 1:
Frau Müller von der Personalabteilung ist glücklich, dass ihr Unternehmen so flexibel ist. Heute steht ein Vorsorgetermin beim Arzt an. Damit sie nicht allzu viel Zeit durch das Hin- und Herreisen verliert, darf sie heute von zu Hause arbeiten. Kein Problem, da kann sie ganz in Ruhe die Lohnbuchhaltung auf die neuen Gehälter ab Januar des nächsten Jahres umprogrammieren. Und tatsächlich arbeitet es sich ohne störende Meetings und Kollegen deutlich leichter und schneller. Zufrieden räumt sie ihren Schreibtisch wieder auf. Dass dabei Dokumente mit Firmeninterna, insbesondere auch Lohlisten ungeschreddert im Papierkorb und am nächsten Tag als Altpapier gebündelt auf der Strasse landen, merkt sie gar nicht ...

Praxisbeispiel 2:
Herr Huber aus dem Verkaufsteam arbeitet drei von fünf Tage mit Homeoffice zuhause. Weil das Wetter so wunderschön ist, setzt er sich in den Garten und arbeitet dort. Zwischendurch telefoniert er mit Kunden, während sein Nachbar im Garten arbeitet und jedes Wort mithört. Gerade spricht er mit einem Kunden über ein Angebot und sie tauschen einige Zahlen aus und verhandeln sogar darüber.

Der Nachbar spitzt die Ohren, denn sein bester Freund arbeitet beim Wettbewerber des Unternehmens von Herrn Huber. Und er erzählt die gerade gehörten Informationen natürlich brühwarm seinem Freund ...

Anforderungen an den Arbeitsplatz

Der Arbeitsplatz für Homeoffice sollte sich in einem separaten Zimmer befinden, sodass man diesen abschliessen kann. Denn auch Familienangehörige sollen keinen Einblick in verarbeitete Personendaten oder in Geschäftsgeheimnisse erhalten. Datenträger und Unterlagen dürfen nie unbeaufsichtigt gelassen werden und gehören nicht in den Wohnbereich. Betriebliche Unterlagen sollten in einem Schrank abgeschlossen aufbewahrt werden, sofern nicht der ganze Raum mit dem Arbeitsplatz abgeschlossen werden kann.

Vertragliche Regelung oder Weisungen des Unternehmens

Datenschutz und Datensicherheit beim Homeoffice sollten zwischen Unternehmen und Arbeitnehmerin bzw. Arbeitnehmer vertraglich geregelt werden. Am besten wird dies – zusammen mit dem Datenschutz und der Datensicherheit am betriebsinternen Arbeitsplatz – in einem besonderen Kapitel des Arbeitsvertrags oder in einer Zusatzvereinbarung zum Arbeitsvertrag (oft Geheimhaltungsvereinbarung genannt) geregelt. Je nach Grösse und Kultur des Unternehmens kann die Regelung allenfalls auch durch Weisungen an die Arbeitnehmerinnen und Arbeitnehmer erfolgen.

Da das Homeoffice oft auch in arbeitsrechtlicher Hinsicht eines Zusatzvertrags zum Arbeitsvertrag bedarf, können Datenschutz und Datensicherheit auch dort geregelt werden.

Das Unternehmen sollte sich in der vertraglichen Regelung unbedingt das Recht ausbedingen, den Arbeitsplatz des Homeoffice in den Privaträumen der Arbeitnehmerin bzw. des Arbeitnehmers inspizieren zu dürfen.

II. Datensicherheit

Datenaustausch/Datentransport

Die Verbindung zum Server des Unternehmens sollte ausschlieslich über ein sogenanntes Virtual Private Network (VPN) hergestellt werden.

Online-Zugänge auf Webdienste oder zu Clouds müssen ebenfalls sicher sein. Der Zugang zu besonders schützenswerten Personendaten des Unternehmens darf nur mit PIN und hardwarebasiertem Vertrauensanker (Zwei-Faktor-Authentifizierung) gewährt werden.

Müssen Personendaten per e-Mail übermittelt werden (z.B. vom Arbeitsgerät des Homeoffice aus an die betriebliche Mailbox), so hat die Übermittlung mit verschlüsseltem E-Mail zu erfolgen. Dabei ist zu beachten, dass auch bei verschlüsselten E-Mails der Betreff und der Absender in der Regel nicht verschlüsselt sind. Die Verschlüsselung der E-Mail und der angehängten Dokumente nützt nichts, wenn der Name der betroffenen Person (z.B. "Arztzeugnis für Hans Muster") erkennbar ist. Berufliche E-Mails sollten nicht an die private Mailbox der Arbeitnehmerin bzw. des Arbeitnehmers übermittelt werden.

Wenn Personendaten nicht elektronisch übermittelt sondern auf Datenträgern transportiert werden, so müssen letztere verschlüsselt bzw. passwortgeschützt sein.

Es dürfen keine betrieblichen Daten auf dafür nicht zugelassenen (privaten) Geräten gespeichert werden – auch nicht vorübergehend.

Backup

Wenn im Betrieb vom Arbeitsplatz aus auf dem Server gearbeitet wird, so findet üblicherweise automatisch ein Backup statt. Das gleiche gilt, wenn über VPN auf den betrieblichen Server gearbeitet wird.

Wenn die Daten lokal auf dem Arbeitsgerät zu Hause gespeichert sind, dann fehlt ein automatisches Backup. in diesen Fällen muss dafür gesorgt werden, dass die betreffenden Dokumente im Sinne eines Backups zusätzlich auf externe mobile Datenträger (z.B. verschlüsselte oder passwortgeschützte USB-Sticks) abgespeichert werden.

III. Arbeitsgeräte

Grundsatz: Arbeitsgeräte werden vom Arbeitgeber zur Verfügung gestellt

Grundsätzlich muss – wie am innerbetrieblichen Arbeitsplatz – das Unternehmen den PC bzw. Laptop und weitere Arbeitsgeräte (z.B. Telefone oder Drucker) für das Homeoffice zur Verfügung stellen. Diese Geräte sollten aus Gründen des Datenschutzes und der Datensicherheit nicht privat genutzt werden. Das Unternehmen sollte dies vertraglich oder durch Weisungen entsprechend regeln.

Ausnahme: Bring Your Own Device (BYOD)

Grundsätzlich sollten keine privaten Geräte im Homeoffice zugelassen werden. Wenn das Unternehmen private Geräte zulässt, so haben wir die gleiche Situation wie im Modus "Bring Your Own Device" (BYOD) am innerbetrieblichen Arbeitsplatz.

Die BYOD-Nutzung ist aus Datenschutzsicht heikel, vor allem was die Datensicherheit und die Abgrenzung zwischen privaten und geschäftlichen Daten betrifft. Die Trennung ist technisch schwierig zu realisieren. Eine logische Abgrenzung ist zudem allenfalls nicht ausreichend, um einerseits die geschäftlichen Daten zu schützen und andererseits den Zugriff auf private Daten durch den Arbeitgeber zu verhindern. Weiter stellen sich Fragen beim Zugriff auf die geschäftlichen Daten durch den Arbeitgeber, zum Beispiel wenn ein Gerät überprüft werden soll oder bei einer Fernwartung. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) empfiehlt deshalb folgendes:

- Klare Nutzungsregelung (Vertrag; schriftliche Weisung), die besagt, was erlaubt ist und was nicht. Für die BYOD-Nutzung gilt aus datenschutzrechtlicher Sicht grundsätzlich das Gleiche wie für die Nutzung der elektronischen Infrastruktur am Arbeitsplatz.
- Trennung von geschäftlichen und privaten Daten (technisch und logisch)
- Gewährleistung der Datensicherheit (z.B. durch Verschlüsselungstechnik, Passwörter etc.)
- Klare Regelung, wo die geschäftlichen Daten gespeichert werden (wenn möglich auf einem Server des Unternehmens)
- Regelung des Zugriffs auf das Gerät durch den Arbeitgeber (z.B. zur Geräteüberprüfung, Fernwartung etc.).

Zusammenfassende Merkpunkte für den Datenschutz im Homeoffice:

- Der Arbeitsplatz sollte sich in einem separaten Zimmer befinden, sodass man diesen abschliessen kann.
- Arbeitnehmende, die mit ihrer Familie oder Mitbewohnern zusammenleben, sollten auch bei kurzzeitigem Verlassen den PC sperren.
- Betriebliche Unterlagen sollten in einem Schrank abgeschlossen aufbewahrt werden.
- Datenträger und Unterlagen dürfen nie unbeaufsichtigt gelassen werden.

.....

- Ausgedruckte Dokumente sind zu vernichten oder ins Unternehmen zurückzubringen.
- Datenträger sind stets nur mit Passwortschutz oder verschlüsselt und Papierunterlagen nur in verschlossenen Behältnissen zu transportieren.
- Werden Laptops, PCs oder sonstige IT-Ausstattung zur Verfügung gestellt, dürfen diese nicht privat genutzt werden.
- Private Hard- und Software sollte grundsätzlich nicht für das Homeoffice eingesetzt werden.
- Es ist untersagt, berufliche E-Mails auf private E-Mail-Postfächer weiterzuleiten.
- (besonders schützenswerte) Personendaten sollen in verschlüsselten Dokumenten und E-Mails ausgetauscht werden.
- Berufliche und private Daten sind zu trennen.
- Die Verbindung zum Server des Unternehmens soll ausschlieslich über ein sogenanntes Virtual Private Network (VPN) erfolgen.
- Zugang zu sensiblen personenbezogenen Daten nur mit PIN und hardwarebasiertem Vertrauensanker (Zwei-Faktor-Authentifizierung).
- Berufliche Telefongespräche sind ausser Hörweite von Dritten zu führen.

Rechtlicher Hinweis:
Recht ist keine exakte Wissenschaft und stetigem Wandel unterworfen. Der Inhalt des Factsheets wurde mit grosser Sorgfalt erarbeitet, trotzdem muss jede Haftung für den Inhalt abgelehnt werden.

Bitte beachten Sie den Aktualitätsstand des Factsheets.