Datenschutz beim HomeOffice / Heimarbeit

(nicht nur während der Kontaktbeschränkungen)

Die folgenden Mindestanforderungen an ein datenschutzgerechtes „Home-Office“ müssen auch in der aktuellen Ausnahmesituation unbedingt eingehalten werden:

Papierunterlagen

- Papierunterlagen müssen sicher transportiert werden. Der Transport von sensitiven personenbezogenen Unterlagen in öffentlichen Verkehrsmitteln darf nur in verschlossenen Behältern vorgenommen werden. Es ist besser, auf ein geschäftliches oder auch privates Fahrzeug auszuweichen.
- Im Home-Office sollen personenbezogene Unterlagen so aufbewahrt werden, dass Unbefugte sie nicht einsehen können. Auch auf Ausdrucke auf einem von mehreren Personen genutzten Drucker ist zu achten. Solange kein separates, abschließbares Zimmer für das Home-Office zur Verfügung steht, gehören die Unterlagen nach Abschluss der Arbeiten zumindest in einen verschlossenen Schrank.
- Personenbezogene Unterlagen, die zu vernichten sind, sollen gesammelt, bei nächster Gelegenheit in das Unternehmen bzw. das Büro mitgenommen und dort der üblichen Vernichtung zugeführt werden. Es kann auch ein heimischer Büro-Aktenvernichter verwendet werden, wenn er das Papier ausreichend klein zerteilt (Partikelschnitt P-4 empfohlen, bei Berufsgeheimnisträgern P-5).

Informationstechnik – Datenspeicher

- Alle mobilen elektronischen Speicher (USB-Sticks, externe Festplatten), auf denen personenbezogene Daten gespeichert werden, sollen verschlüsselt werden. Alle üblichen Betriebssysteme bieten hierfür unmittelbar anwendbare Funktionen an. Bei Windows 10 heißt die Technik Bitlocker. Auch spezielle Software, z. B. Veracrypt, ist gut geeignet. Für Speicher, die Datensicherungen aufnehmen, kann auch auf die Verschlüsselungsfunktion der jeweiligen Sicherungssoftware zurückgegriffen werden, wenn sie dem Stand der Technik entspricht.
- Laptops, Tablets und Smartphones benötigen einen starken Passwortschutz und verschlüsselten Speicher.
- Berufliche Daten über Beschäftige und Dritte, die über Kontaktdaten hinausgehen, dürfen auf privaten Geräten allenfalls kurzzeitig gespeichert werden. Sensible Daten gehören auf geschäftliche Geräte.
- Derartige Daten oder personenbezogene Daten in großem Umfang sollten nicht auf Geräten im Home-Office, sondern direkt auf Servern im Unternehmen bzw. in der Behörde gespeichert werden. Dafür empfiehlt sich die Arbeit direkt auf diesen Servern über einen geschützten Fernzugriff.
- Die Speicherung kann auch ein zuverlässiger Dienstleister übernehmen, wenn er datenschutzgerecht beauftragt wurde. Der Dienstleister sollte die Daten in der EU oder in einem als gleich sicher geltenden Land speichern und auch dort seinen Sitz haben.[1] Auch hier ist eine Verschlüsselung vorzusehen. Bei sensitiven Daten sollte das Unternehmen allein über den Schlüssel zum Entschlüsseln verfügen. Liegt der Schlüssel in der Hand der bzw. des Beschäftigten, sollte er diesen im Unternehmen hinterlegen.

LBC Management Support GmbH Gohliser Straße 6 04105 Leipzig Geschäftsführer Lars Bosse T +49/ 341/ 5861 9451 DSB@LBC.Management www.LBC.Management

Informationstechnik – Geräte

- Soweit private Geräte zum Einsatz kommen, sollen private und berufliche Daten voneinander getrennt werden. Auf Computern sollten je ein Konto für private und für berufliche Zwecke eingerichtet werden. Für Smartphones und Tablets stellen die Betriebssystemhersteller entsprechende Techniken zur Verfügung. Wem die Einrichtung zu kompliziert erscheint, der verwendet am Besten separate Geräte.
- Sensitive personenbezogene Daten (z. B. Daten zur Gesundheit, zu politischen oder weltanschaulichen Ansichten, zur Gewerkschaftszugehörigkeit oder sexuellen Orientierung) dürfen auch in der derzeitigen Notsituation nur auf geschäftlichen Geräten verarbeitet werden.
- Bildschirme müssen so aufgestellt werden, dass sie nicht durch Unbefugte eingesehen werden können.
- Es sind regelmäßig Datensicherungen vorzunehmen.

Informationstechnik – Netze

- Das im Home-Office genutzte WLAN muss mit einem nicht erratbaren Passwort (mit den Verfahren WPA2 oder, besser, WPA3) verschlüsselt werden.
- Der private Internetanschluss kann mitverwendet werden. Der verwendete Computer soll über ein Virtuelles Privates Netz (VPN) mit dem Unternehmensnetz verbunden werden. Das muss von dem Router unterstützt werden, mit dem das Unternehmen an das Internet angeschlossen wird. Kleine Unternehmen können entsprechende Funktionen ihrer Router nutzen. Geeignete Geräte sind preiswert am Markt erhältlich.

Informationstechnik – Sicherheit

- Es sollten keine Zugriffe von außen auf Informationstechnik in der zur Arbeit genutzten Wohnung zugelassen werden. Die Router, die den Internetanschluss bereitstellen, verfügen in der Regel über eine einfache Firewall, die solche Zugriffe unterbindet.
- Beim Öffnen von Links und Dokumenten in unerwarteten Nachrichten ist besondere Vorsicht geboten. Viele Schutzmaßnahmen, die innerhalb des Netzwerks des Unternehmens greifen, stehen zuhause nicht zur Verfügung. Programme zur Bekämpfung von Schadsoftware (Anti-Viren-Programme) sind auf allen Computern Pflicht, reichen jedoch nicht aus, um alle Angriffe zu erkennen. Dies hat sich besonders deutlich bei der letzten Welle von Infektionen durch Erpressungstrojaner gezeigt. Deswegen bedarf es eines gesunden Misstrauens der Beschäftigten.
- Private und unternehmerische Datenträger sind zu trennen. Geschäfts-Computer und Smartphones sollten nur mit geschäftlichen Datenträgern verbunden werden und umgekehrt. Daten aus dem Home-Office sollen über eine sichere Netzverbindung in das Büro übermittelt werden, nicht über Datenträger.

- Auf geschäftlichen Geräten kann Raum für die private Nutzung eingeräumt werden. Welche Beschränkungen diesem Raum auferlegt werden müssen, hängt von dem Schutzbedarf der beruflich verarbeiteten Daten ab.
- Arbeitgeber dürfen jedoch keinen Zugriff auf private Geräte ihrer Beschäftigte nehmen. Zulässig ist es, die Verwendung privater Geräte für geschäftliche Zwecke (zur Verarbeitung nicht sensibler Daten) an einfache, sicherheitsrelevante Bedingungen (z. B. eine aktuelle Version des Betriebssystems) zu knüpfen und die Einhaltung dieser Bedingungen ohne Zugriff auf personenbezogene Daten zu überprüfen.

Kommunikationstechnik

Telefonie

- Es ist datenschutzrechtlich am Sichersten, ausschließlich geschäftlich gestellte Telefone zu verwenden.
- Wer mit Dritten in deren beruflicher Tätigkeit in Kontakt steht, kann – in vom Arbeitgeber gesetzten Grenzen – deren Kontaktdaten auch in einem privaten Gerät speichern. Sofern diese Kontaktdaten nicht öffentlich zugänglich sind und im Telefonbuch gespeichert werden, ist Sorge zu tragen, dass auf das Telefonbuch nicht durch Dritte, z. B. durch Hersteller von auf dem Gerät installierten Apps, zugegriffen werden kann.
- Kontaktdaten von Privatpersonen, bei denen bereits der Umstand, dass Kontakt besteht, sensibel zu behandeln ist, gehören jedoch ausschließlich auf Geschäftsgeräte.
- Telefone speichern üblicherweise Angaben über die geführten Telefongespräche. Diese sind in regelmäßigen Abständen zu löschen.

Messenger

- Es können alle Messenger verwendet werden, die eine Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik bieten und deren Betreiber keine Angaben über die gesendeten und empfangenen Nachrichten oder die Nutzung der App für eigene Zwecke verarbeiten (diese Anforderungen erfüllt z.B. WhatsApp nicht). Werden diese Umstände aus den Datenschutzerklärungen eines Betreibers nicht deutlich, ist dessen Dienst voraussichtlich für die Nutzung nicht geeignet.
- Ein Arbeitgeber kann die Verwendung eines Messengers auf einem privaten Gerät nicht verlangen, der zwangsweise Zugriff auf das Telefonbuch des Geräts nimmt.
- Die Übermittlung sensibler Daten mit einem Messenger ist nur unter eingeschränkten Bedingungen zulässig.

Videotelefonie und -konferenzen

- Videotelefonie und Videokonferenzen sollen über verschlüsselte Kanäle abgewickelt werden. Dies betrifft sowohl die Vermittlung als auch die Übertragung der Ton- und Bilddaten. Bei der Videotelefonie soll dies eine Verschlüsselung von Ende zu Ende bewirken.
- Die Bereitstellung des Videokonferenzdienstes kann ein zuverlässiger Dienstleister übernehmen, wenn er datenschutzgerecht beauftragt wurde und der Betreiber keine Angaben über die Beschäftigten und deren Kommunikation oder die Nutzung der Software für eigene Zwecke verarbeitet. Der

Dienstleister sollte die Daten in der EU oder in einem als gleich sicher geltenden Land speichern und auch dort seinen Sitz haben.

- Da eine Ende-zu-Ende-Verschlüsselung bei einer Videokonferenz mit mehr als zwei Teilnehmern vielfach nicht möglich ist, wird empfohlen, nur Anbieter in EU, EFTA und der Schweiz zu verwenden, wenn innerhalb der Videokonferenz sensible Daten besprochen werden sollen. Berufsgeheimnisträger dürfen nur Dienstleister einsetzen, die bei einem Vertraulichkeitsbruch strafrechtlich belangt werden können.
- Am besten (wenn auch oft nicht mit verhältnismäßigem Aufwand leistbar) ist die Bereitstellung eines eigenen Dienstes mit öffentlich verfügbarer Software.
- Alternativ sollte überlegt werden, ob anstelle einer Videokonferenz auch eine Telefonkonferenz ausreichen könnte, um die gewünschte Abstimmung untereinander herbeizuführen. Diese kann sehr viel leichter datenschutzgerecht durchgeführt werden.

Organisatorische Regelungen

Jedes Unternehmen sollte Regelungen zu Datenschutz und Sicherheit im Home-Office treffen und den Beschäftigten verständlich und nachvollziehbar erläutern. Als Hilfestellung können die Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) „Home Office? – Aber sicher!“und die vom Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) im letzten Jahr veröffentlichte Information „Telearbeit und Mobiles Arbeiten“[5] herangezogen werden.

In den Regelungen sollten die Kontaktdaten von Personen aufgeführt werden, die in datenschutzrechtlichen Zweifelsfällen oder bei informationstechnischen Problemen Hilfestellung geben. Es sollte auch erläutert werden, wie vorzugehen ist, wenn eine Verletzung des Schutzes personenbezogener Daten vermutet wird.

Vor allem diejenigen Berufsgruppen, die mit besonders sensiblen Daten arbeiten, beispielsweise im medizinischen Kontext oder bei psychologischen Beratungen, sollten in besonderer Weise auf die Einhaltung datenschutzrechtlicher Grundsätze achten. Die Nutzung von Plattformen etwa zur videogestützten Online-Beratung beinhaltet oft eine Vielzahl von Risiken, die sorgsam mit den Vorteilen abgewogen werden müssen. Vor dem Kauf oder Einsatz von Videokonferenztechnik kann eine Datenschutzfolgenabschätzung nötig sein, die Zusammen mit den Datenschutzbeauftragten erstellt wird.

Fazit

Auch in dieser Zeit einer extrem beschleunigten und teilweise auch überstürzten Digitalisierung der Arbeitswelt muss der Schutz personenbezogener Daten immer mitgedacht werden. Dort, wo die Dringlichkeit der aktuell zu ergreifenden Maßnahmen dies nicht im notwendigen Umfang zulässt, muss kontinuierlich nachgebessert werden. Sollten datenschutzrechtliche Unwägbarkeiten oder gar Missstände auftreten, sind diese umgehend zu beheben.

Lars Bosse

Datenschutzbeauftragter und -auditor (TÜV)

Stand: 05.05.2020

LBC Management Support GmbH Gohliser Straße 6
04105 Leipzig
Geschäftsführer Lars Bosse
T +49/ 341/ 5861 9451
DSB@LBC.Management
www.LBC.Management