STIFTUNG DATENSCHUTZ

DATENSCHUTZ IM HEIMBÜRO

EINE HANDREICHUNG

THEMEN

Dieses Merkblatt richtet sich an Arbeitgeber und Beschäftigte in kleinen und mittelständischen Unternehmen, die infolge der Corona-Pandemie im Heimbüro arbeiten. In der Praxis hat sich gezeigt, dass viele betroffenen Unternehmen auch nach Monaten des häuslichen Arbeitens noch keine umfassenden betrieblichen Vereinbarungen getroffen haben, die neben den zweifellos wichtigen Schwerpunkten des Datenschutzes und der Datensicherheit auch andere Aspekte wie den Arbeits- und Gesundheitsschutz oder den Ausgleich für höhere häusliche Aufwendungen umfassen.

Daher soll dieses Merkblatt pragmatische, praxisbezogene Hilfestellung leisten, wie personenbezogene Daten auch im Heimbüro geschützt werden können; die umfassende Vorbereitung auf einen längerfristigen Umzug ins Heimbüro ersetzt es jedoch nicht. Auch Datenverarbeitungen in Behörden, die gesonderten Vorschriften unterliegen, sind hier nicht erfasst. Grundsätzliche Hinweise zur Verarbeitung personenbezogener Daten gibt die Broschüre „Datenschutz im Betrieb – Was Beschäftigte wissen müssen“, an die dieses Merkblatt anschließt.

ORGANISATORISCHES

Die Datenverarbeitung im Heimbüro unterliegt den gleichen Vorschriften, die auch am betrieblichen Arbeitsplatz gelten. Dies ist unter den gegenwärtigen Bedingungen auch bei bestem Wollen nicht immer vollständig zu gewährleisten. Dennoch müssen sich Arbeitgeber wie Beschäftigte auch unter diesen widrigen Umständen bemühen, personenbezogenen Daten vorschriftsmäßig zu schützen.

Unabhängig davon, ob die Arbeit am betrieblichen oder am häuslichen Arbeitsplatz stattfindet, ist der Arbeitgeber datenschutzrechtlich Verantwortlicher im Sinne der Datenschutz-Grundverordnung.

Daher müssen Arbeitgeber die Beschäftigten zum Umgang mit personenbezogenen Daten in der Telearbeit gesondert anweisen und in Bezug auf Vorsichtsmaßnahmen schulen. Dies sollte zu Nachweiszwecken dokumentiert werden. Idealerweise regelt dies die Unternehmensleitung in einer mit dem Betriebsrat abgestimmten Betriebsvereinbarung.

Das Unternehmen haftet als Verantwortliche Stelle auch für das Fehlverhalten von Beschäftigten; eine persönliche Haftung ist nur in Ausnahmefällen denkbar. Bei persönlichem Verschulden kann aber auch der Arbeitgeber die Beschäftigten in Regress nehmen, wenn beispielsweise wegen schwerer Datenschutzverstöße, die ein Beschäftigter vorsätzlich begangen hat, gegen den Arbeitgeber ein Bußgeld verhängt wird.

Die Meldepflicht von Datenschutzverstößen besteht auch am häuslichen Arbeitsplatz. Mehr dazu in „Datenschutz im Betrieb – Eine Handreichung für Beschäftigte“.

ARBEITSPLATZ, COMPUTER, DATENTRÄGER

Da die wenigsten Beschäftigten über ein eigenes, abschließbares Arbeitszimmer verfügen, sollte zumindest der Arbeitsplatz so gestaltet sein, dass ein möglichst störungsfreies Arbeiten gewährleistet ist, ohne dass Haushaltsangehörige (oder Haustiere) Zugang zum Computer, zu Datenträgern und Papieren haben, und ohne dass sie Telefonate/Videokonferenzen mit vertraulichen Inhalten mithören können. Dienstliche Telefonate sollten also nicht vom Balkon oder Garten aus geführt werden.

Arbeitsunterlagen sollten außerdem verschlossen (abschließbarer Schrank, Schreibtischschublade) aufbewahrt werden. Außerdem sind nicht mehr benötigte Unterlagen datenschutzgerecht zu vernichten. Listen mit Kundendaten gehören nicht ins Altpapier, sondern müssen sicher aufbewahrt und bei nächster Gelegenheit ins Büro mitgenommen und dort vernichtet werden. Geeignet wäre auch ein Aktenvernichter mit ausreichend kleinem Partikelschnitt (mind. P-4).

Der besondere Schutz von Datenträgern und Unterlagen muss natürlich auch während des Transports gewährleistet sein, etwa zwischen Heimbüro und Arbeitsstelle bei alternierender Telearbeit. Arbeitgebern sollten die Kosten für Taxi oder Mietwagen übernehmen, damit besonders sensible Daten nicht per ÖPNV transportiert werden müssen.

Idealerweise stattet der Arbeitgeber die Beschäftigten für die Arbeit außerhalb der Betriebsstätte mit eigener Hardware aus, die durch Virenschutz, Firewalls, Passwörter und Verschlüsselung nach dem betrieblichen Standard geschützt ist. Ist dies (kurzfristig) nicht möglich, und die Beschäftigten erklären sich im eigenen Interesse bereit, vorübergehend ihre eigene Infrastruktur einzusetzen, gilt weiterhin der Grundsatz, Privates und Berufliches zu trennen.

Der Computerbildschirm muss beim Verlassen des Arbeitsplatzes gesperrt werden; Computer und Datenträger wie Festplatten und USB-Sticks sollten verschlüsselt werden.

Insgesamt gilt:

- möglichst VPN nutzen
- bei einem privaten Internetzugang sollte der Computer entweder durch ein Kabel oder durch ein verschlüsseltes WLAN verbunden sein
- möglichst keine private und dienstliche Hardware miteinander verbinden
- auf privaten Rechnern ein eigenes Nutzerprofil einrichten, dass nur für die betrieblichen Aufgaben genutzt wird
- dienstliche Daten in einem verschlüsselten Bereich speichern
- gegebenenfalls den Bildschirm mit einer Sichtschutzfolie versehen
- keine Smart-Home-Geräte im Arbeitszimmer nutzen
- keine dienstlichen Daten über private Accounts austauschen (E-Mail, Messenger)

KOMMUNIKATION

Auch hier ist der Grundsatz der Trennung von beruflichen und privaten Daten zu berücksichtigen. Daher sollten keine privaten Accounts (E-Mail, Messenger, Videokonferenzsysteme) genutzt werden. Falls einmal Daten von dienstlichen Kontakten auf privaten Telefonen landen sollten, müssen diese kurzfristig gelöscht werden; es muss vermieden werden, dass diese an Anbieter von privat genutzten Diensten, zum Beispiel Messengern, weitergegeben werden. Wer das private Telefon für dienstliche Gespräche nutzen muss, sollte seine Rufnummer unterdrücken.

Arbeitgeber sollten mit Anbietern von Messenger- und/oder Videokonferenzsystemen Verträge abschließen, welche die Datenverarbeitung regeln, gegebenenfalls auch in Auftragsverarbeitungsverträgen. Dabei sollten Betriebsrat und Datenschutzbeauftragte, wenn vorhanden, beteiligt werden.

Der Arbeitgeber darf nicht verlangen, dass Beschäftigte invasive Programme oder Apps auf ihren privaten Endgeräten installieren. Das gilt auch und insbesondere für Software, die Überwachungsfunktionen mitbringt. Diese verstoßen praktisch immer gegen gesetzliche Vorschriften.

Besonders Videokonferenzplattformen standen zu Beginn der Pandemie in der Kritik. Inzwischen gibt es zuverlässige Alternativen in Deutschland – wie auch für Messenger- und Cloud-Dienste. (siehe Weiterführende Informationen)

SONSTIGES

Arbeitgeber verantworten die Verarbeitung personenbezogener Daten auch im Heimbüro. Sie bestimmen, welche Daten verarbeitet werden und welche Werkzeuge sie den Beschäftigten zur Verfügung stellen. Daher obliegt es ihnen, die datenschutzrechtlichen Vorschriften zu akzeptieren und die Privatsphäre von Kunden und Beschäftigten zu schützen, indem sie Dienste verwenden, die den Anforderungen der Datenschutz-Grundverordnung entsprechen. Das betrifft Messenger-Dienste ebenso wie Cloud-Speicher und Videokonferenz-Plattformen sowie viele andere Software-Werkzeuge.

Als zu Beginn der Pandemie für viele Beschäftigte kurzfristig die Möglichkeit der Arbeit im häuslichen Umfeld geschaffen wurde, mussten zwangsläufig viele Kompromisse eingegangen werden. Je länger die Situation andauert, umso mehr sollten nun verbindliche Vereinbarungen getroffen und die Heimarbeitsplätze langfristig mit der notwendigen Infrastruktur ausgestattet werden. Absprachen und Anweisungen sollten schriftlich niedergelegt und gegebenenfalls in individuellen bzw. betrieblichen Vereinbarungen dokumentiert werden. Die sichere Verarbeitung von personenbezogenen Daten im Heimbüro erfordert ein umfassendes Konzept, das mit Hilfe von Datenschutz-Spezialisten erstellt werden sollte.

WEITERFÜHRENDE INFORMATIONEN (LINKS)

Zahlreiche Links zu Handreichungen und Checklisten des Bundesamts für die Sicherheit in der Informationstechnik, der Datenschutzaufsichtsbehörden des Bundes und der Länder bei der Gesellschaft für Datenschutz und Datensicherheit

→ **sds-links.de/3zf**

Zur Verarbeitung von personenbezogenen Daten am Arbeitsplatz: **„Datenschutz im Betrieb – Eine Handreichung für Beschäftigte“**

→ **sds-links.de/DSimBetrieb**

Hinweise zu US-Anbietern
der Landesdatenschutzbehörde Rheinland-Pfalz

→ **sds-links.de/x16**

Orientierungshilfe zu Videokonferenzsystemen
der Datenschutzkonferenz

→ **sds-links.de/vet**

IMPRESSUM

Herausgeber
Stiftung Datenschutz

Autorinnen
Prof. Dr. Anne Riechert
Antje Simon, M.A.

Version
1.0, Stand Januar 2021