Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Telearbeit und Mobiles Arbeiten

Ein Datenschutz-Wegweiser

Inhalt

Was ist Telearbeit?

Bei der Telearbeit wird die Arbeitsleistung im Wechsel zwischen dem Arbeitsplatz in der Dienststelle und im häuslichen Bereich der Beschäftigten erbracht (Telearbeitsplatz). Die häusliche Arbeitsstätte ist dabei durch elektronische Informationsverarbeitungs- und Kommunikationsmittel mit der Dienststelle verbunden.

Was ist Mobiles Arbeiten?

Das „Mobile Arbeiten“ ermöglicht im Unterschied zur Telearbeit ortsunabhängiges Arbeiten. Mit Hilfe mobiler Informations- und Kommunikationstechnik wird ein Fernzugriff auf die eigene behördeninterne IT-Infrastruktur hergestellt. Im Rahmen des Arbeits- oder Dienstverhältnisses trägt der Arbeitgeber die datenschutzrechtliche Verantwortung für die Datenverarbeitung bei Telearbeit und Mobilem Arbeiten.

Sind Telearbeit und Mobiles Arbeiten mit dem Datenschutz vereinbar?

Der Datenschutz schließt Telearbeit und Mobiles Arbeiten nicht grundsätzlich aus. Eine klare gesetzliche Regelung für die datenschutzrechtliche Zulässigkeit von Telearbeit und Mobilem Arbeiten gibt es indes nicht. Es sollte deshalb in jedem Einzelfall unter Berücksichtigung der Art der zu verarbeitenden Daten und ihres Verwendungszusammenhangs sorgfältig und differenziert geprüft werden, ob die Wahrnehmung der jeweiligen Aufgaben oder Tätigkeiten im Rahmen von Telearbeit und Mobilem Arbeiten datenschutzrechtlich vertretbar ist. Die Entscheidung muss der Arbeitgeber treffen.

Dabei ist zu berücksichtigen, dass die Verlagerung von Tätigkeiten in Telearbeit oder Mobiles Arbeiten, bei denen personenbezogene Daten verarbeitet werden, Risiken für die Persönlichkeitsrechte dieser Personen birgt. Denn Datenmissbrauch oder eine unzulässige Einflussnahme durch Dritte sind – auch wegen der eingeschränkten Kontroll- und Einflussmöglichkeiten des Arbeitgebers – leichter möglich.

Vorsicht bei besonders schützenswerten Daten!

Die Risiken bei Telearbeit und Mobilem Arbeiten lassen sich in der Praxis nicht gänzlich vermeiden. Sie sind bei besonders schützenswerten personenbezogenen Daten nur dann vertretbar, wenn deren Schutz durch angemessene technisch-organisatorische Maßnahmen und entsprechende Kontrollmöglichkeiten des Arbeitgebers gewährleistet ist.

Welche Daten sind besonders schützenswert?

Beschäftigtendaten

Arbeitgeber sammeln im Laufe eines Berufslebens eine Fülle von persönlichen Daten über ihre Beschäftigten, die ein umfassendes Bild über die Betroffenen geben. Diese Daten bedürfen deshalb nach § 26 Bundesdatenschutzgesetz (BDSG) eines besonderen Schutzes und unterliegen oftmals dem Personalaktengeheimnis.

Sozialdaten

Als besonders schützenswert sind auch personenbezogene Daten anzusehen, welche die gesetzlichen Sozialversicherungsträger (Kranken- und Pflegekassen, Renten-, Unfallversicherungsträger, Bundesagentur für Arbeit, Jobcenter) zur Aufgabenerfüllung über ihre Mitglieder bzw. Versicherten speichern. Diese Sozialdaten i. S. d. § 67 Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) unterliegen dem Sozialgeheimnis nach § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I). Das Sozialgeheimnis verpflichtet Sozialversicherungsträger dafür Sorge zu tragen, dass Daten nur Befugten zugänglich sind. Es umfasst gleichzeitig den Anspruch

der Betroffenen auf Unterlassen einer unbefugten Verarbeitung der sie betreffenden Sozialdaten.

Besondere Kategorien personenbezogener Daten

Zu den besonders schützenswerten personenbezogenen Daten gehören vor allem die in Art. 9 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) genannten Angaben zur rassischen und ethnischen Herkunft, Gewerkschaftszugehörigkeit, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die DSGVO verwendet hierfür den Begriff der besonderen Kategorie personenbezogener Daten.

Unterschiede auch bei besonderen Kategorien personenbezogener Daten

Bei der Entscheidung, ob und ggf. unter welchen Vorkehrungen sich bestimmte Aufgaben für Telearbeit und Mobiles Arbeiten eignen, gilt es jedoch hinsichtlich des Umgangs mit besonderen Kategorien personenbezogener Daten zu differenzieren.

Auch hier ist im Einzelfall zu entscheiden, ob das Risiko für einen Datenmissbrauch angemessen reduziert werden kann oder ob das unvermeidbare Restrisiko eine Datenverarbeitung im Rahmen von Telearbeit oder Mobilem Arbeiten ausschließt.

Grundsatz: Je sensibler und damit schützenswerter personenbezogene Daten sind, desto stärker sind sie zu schützen.

Risiken bei den Arbeitsabläufen

Bei der Bewertung, ob und ggf. unter welchen Umständen für eine bestimmte Tätigkeit Telearbeit oder Mobiles Arbeiten in Betracht kommen, muss auch berücksichtigt werden, wie hoch das Risiko eines Missbrauchs im Umgang mit personenbezogenen Daten angesichts der gegebenen konkreten Arbeitsabläufe einzustufen ist.

Telearbeit und Mobiles Arbeiten sollten grundsätzlich als eine voll elektronische Datenverarbeitung ohne Medienbruch ausgestaltet werden. D.h., die schriftliche Kommunikation mit dem Arbeitgeber, die Entgegennahme von Aufgaben, der Umgang mit personenbezogenen Daten und die Übermittlung der Arbeitsergebnisse sollten automatisiert mit Hilfe von IT-Einrichtungen und über verschlüsselte elektronische Kommunikationswege stattfinden. Dadurch entfällt die Notwendigkei Unterlagen zu transportieren, was ein hohes Risiko des Verlusts, der Beschädigung sowie der unbefugten Kenntnisnahme birgt.

Bei medienbruchfreier Gestaltung birgt Telearbeit ein geringeres Missbrauchsrisiko als das Mobile Arbeiten. Im Gegensatz zu Mobilem Arbeiten kann der Arbeitsplatz bei der Telearbeit vom Arbeitgeber / von der Dienststelle kontrolliert und Risiken minimiert werden.

Mobiles Arbeiten birgt hingegen immer das Risiko des Verlustes des mobilen Gerätes. Dieses Risiko kann allerdings reduziert werden, wenn die Daten auf dem mobilen Gerät verschlüsselt werden und der Transport des mobilen Gerätes nur im gesperrten Zustand erfolgt. Zur Authentifizierung eingesetzte, hardwarebasierte Vertrauensanker wie Sicherheitskarten sollten getrennt von dem mobilen Gerät aufbewahrt werden.

Öffentliche Netzwerkzugänge (offene Internetzugänge z.B. im Flugzeug, Zug oder Hotel) dürfen über mobile Geräte nur genutzt werden, wenn ein Zugriff auf die firmen-/behördeninterne Infrastruktur über ein sogenanntes Virtual Private Network (VPN) erfolgt, das die Verbindung zum firmen-/behördeninternen Netz durch eine ausreichend starke Verschlüsselung schützt.

Beim mobilen Arbeiten im öffentlichen Bereich (z.B. Zug, Flughafen etc.) sollte der mobil Arbeitende außerdem darauf achten, dass der Bildschirm und die Tastatur der genutzten mobilen Geräte durch Passanten und Videokameras nicht einzusehen ist.
Dienstliche Telefonate mit Personenbezug sollten, wie vertrauliche dienstliche Gespräche, im öffentlichen Raum nur geführt werden, wenn ein Mithören ausgeschlossen werden kann.

Bei einer Datenverarbeitung im Auftrag (Art. 28 DSGVO; § 80 SGB X) muss der Auftragnehmer sicherstellen, dass im Falle von Telearbeit und / oder Mobilem Arbeiten der Datenschutz gewahrt wird und die Kontrollrechte – auch für die Aufsichtsbehörde – gewährleistet sind.

Datensicherheit beim IT-Einsatz

Um Mobiles Arbeiten und Telearbeit – soweit dabei mobile Geräte genutzt werden – datensicher zu gestalten, empfiehlt der BfDI nur Geräte einzusetzen, die durch das Bundesamt für die Sicherheit in der Informationstechnik für das Mobile Arbeiten in der Bundesverwaltung zugelassen wurden.

Das Risiko kann darüber hinaus minimiert werden, wenn durch den Arbeitgeber im Rahmen der erforderlichen technisch-organisatorischen Maßnahmen (Art. 32 DSGVO) zumindest die folgenden Vorgaben erfüllt sind:

- Zugang der Berechtigten zu den sensiblen personenbezogenen Daten nur mit PIN und hardwarebasiertem Vertrauensanker (Zwei-Faktor-Authentifizierung).

- Verbindung ausschließlich über ein sogenanntes Virtual Private Network (VPN).
- Verschlüsselung der Daten (Ende-zu-Ende-Sicherheit) inkl. Ablageverschlüsselung auf dem mobilen Gerät.
- Sperrung von USB-Zugängen und anderen Anschlüssen.
- Keine Anbindung von Druckern.
- Keine private Nutzung der beruflich zur Verfügung gestellten IT-Ausstattung.
- Regelmäßige Schulung / Fortbildung der Beschäftigten zum datensicheren und datenschutzgerechten Umgang mit mobilen Geräten.

Weitere Hinweise zu datensicherem Mobilen Arbeiten finden sich in der Broschüre „Sicheres mobiles Arbeiten“ des Bundesamtes für Sicherheit in der Informationstechnik, abrufbar unter:

https://www.bsi.bund.de/DE/Publikationen/Broschueren/broschueren_node.html

Sicherer Transport von Unterlagen und Datenträgern

Müssen bei Telearbeit oder Mobilem Arbeiten Unterlagen oder Datenträger (CDs, USB-Sticks etc.) von den Beschäftigten transportiert werden, so ist auch hierbei mit vielerlei Gefahren zu rechnen, die zu Verlust oder Beschädigung der Daten führen können. Deshalb sind bei diesem Transport folgende Mindestanforderungen zu gewährleisten:

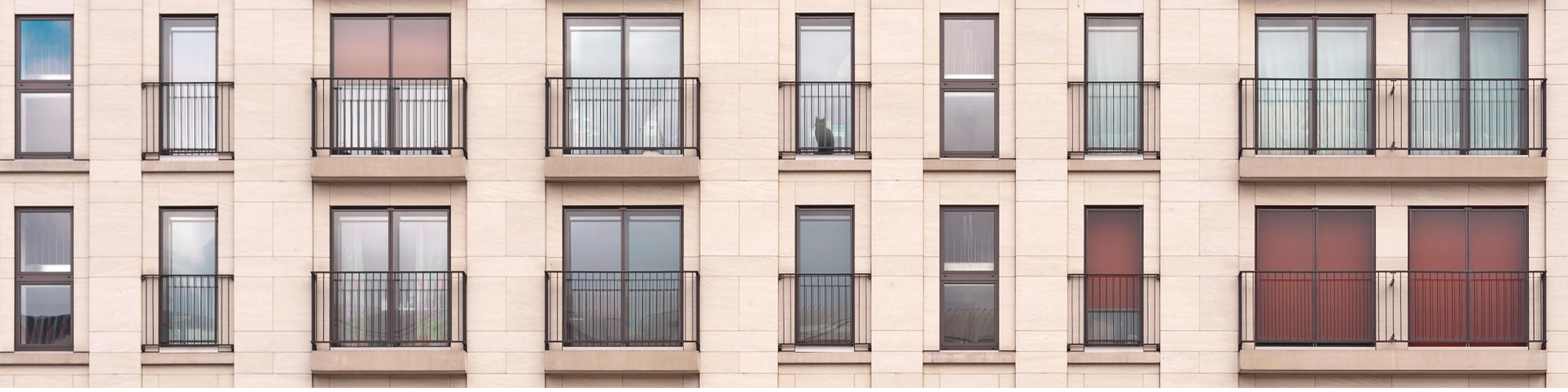
- Datenträger sind stets nur verschlüsselt und Papierunterlagen nur in verschlossenen Behältnissen zu transportieren,
- Datenträger und Unterlagen dürfen nie unbeaufsichtigt gelassen werden.

Kontrollrechte und -pflichten

Da letztendlich die Arbeitgeber die Verantwortung für die personenbezogenen Daten tragen, genügt es nicht, nur technisch-organisatorische Vorgaben zu treffen. Vielmehr hat der Arbeitgeber / Dienstherr nicht nur das Recht, sondern auch die Pflicht, vor und nach der Genehmigung von Telearbeit oder Mobilem Arbeiten routinemäßig und in regelmäßigen Abständen zu kontrollieren, ob die Vorgaben eingehalten werden.

Dies gilt insbesondere, wenn besonders schutzwürdige Daten durch Telearbeit oder Mobiles Arbeiten verarbeitet werden sollen.

Es muss durch geeignete technische und organisatorische Maßnahmen sichergestellt werden, dass der Arbeitgeber eine datenschutzwidrige Nutzung des mobilen Gerätes entdecken kann, z.B. durch Protokollierung. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt zudem den Einsatz eines Mobile Device Managements.



Im Rahmen von Telearbeit muss der Arbeitgeber darüber hinaus die Möglichkeit des Zugangs zur Wohnung des Beschäftigten haben. Art. 13 Grundgesetz (GG) garantiert jedoch die Unverletzlichkeit der Wohnung. Zwar gilt Art. 13 GG zwischen Privaten nicht unmittelbar. Die Grundrechte beeinflussen aber als objektive Wertordnung auch das Privatrecht, so dass Art. 13 GG Arbeitnehmern jedenfalls mittelbar Schutz gewährt. Insoweit besteht hier ein Spannungsverhältnis. Dieses kann aufgrund der Bedeutung des Art. 13 GG nicht dadurch gelöst werden, in der Vereinbarung von Telearbeit eine stillschweigende Zustimmung zum Betreten der Wohnung zu sehen. Das notwendige Zutrittsrecht des Arbeitsgebers / Dienstherrn muss daher vertraglich mit dem in Telearbeit Beschäftigten vereinbart werden, wobei auch das Einverständnis der in häuslicher Gemeinschaft mit ihm zusammenlebenden Personen umfasst sein muss. Die sonstigen Kontrollberechtigten, wie z. B. der betriebliche oder der behördliche Beauftragte für den Datenschutz, sollten in das Zutrittsrecht einbezogen werden.

Weitere datenschutzrechtliche Empfehlungen

- Verantwortlichkeiten im Umgang mit personenbezogenen Daten sind umfassend vertraglich festzulegen.
- Eine private Nutzung der vom Arbeitgeber zur Verfügung gestellten IT-Ausstattung ist nicht zulässig.
- Private Hard- und Software dürfen für Telearbeit und das Mobile Arbeiten nicht eingesetzt werden.
- Berufliche E-Mails dürfen nicht auf private Postfächer der mobil Arbeitenden umgeleitet werden.
- Bei der Telearbeit müssen, wenn diese nicht ausschließlich medienbruchfrei erfolgt, geeignete häusliche Räumlichkeiten und Arbeitsmittel zur sicheren Aufbewahrung und vertraulichen Behandlung von Unterlagen und Datenträgern mit personenbezogenen Daten vorhanden sein. Auch die mit dem in Telearbeit Arbeitenden in häuslicher Gemeinschaft lebenden Personen dürfen keinen Zugriff auf betriebliche / dienstliche Unterlagen haben.
  Die hierfür erforderlichen Sachmittel sind vom Arbeitgeber zur Verfügung zu stellen, wenn sie nicht bereits vorhanden sind.

- Die Datenschutzgrundsätze für Telearbeit und Mobiles Arbeiten sind in einer Betriebs-/Dienstvereinbarung festzuschreiben.
- Bei der Entscheidung, ob sich Tätigkeiten für Telearbeit und / oder Mobiles Arbeiten eignen, ist der/die betriebliche oder behördliche Datenschutzbeauftragte rechtzeitig zu beteiligen.
- Bei der Einrichtung eines Telearbeitsplatzes soll der/die betriebliche oder behördliche Datenschutzbeauftragte eingebunden werden. Er/Sie kann allgemeine oder konkrete Vorgaben machen. Dem/Der Datenschutzbeauftragten sind die erforderlichen Kontrollrechte einzurichten.

Herausgeber:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

Tel. +49 (0) 228 99 77 99-0
Fax +49 (0) 228 99 77 99-5550
E-Mail: arbeitsgruppe12b@bfdi.bund.de
Internet: www.bfdi.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: dreamstime, fotolia, iStockphoto, Adobe Stock, getty

Stand: Januar 2019