Telearbeit und Mobiles Arbeiten

Ein Datenschutz-Wegweiser

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Inhalt

1 Was ist Telearbeit?

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

2 Was ist Mobiles Arbeiten?

Das „Mobile Arbeiten“ ermöglicht im Unterschied zur Telearbeit orts-unabhängiges Arbeiten. Mit Hilfe mobiler Informations- und Kommuni-kationstechnik wird ein Fern-zugriff auf die IT-Infrastruktur des Arbeitgebers/Dienstherrn hergestellt. Im Rahmen des Arbeits- oder Dienstverhältnisses trägt der Arbeitgeber/Dienstherr die datenschutzrechtliche Verantwortung für die Datenverarbeitung bei Telearbeit und Mobilem Arbeiten.

3 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 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 endgültige Entscheidung darüber muss der Arbeitgeber/Dienstherr treffen.

Wenn es beim Einsatz von Telearbeit oder Mobilem Arbeiten zur Verarbeitung von personenbezogenen Daten kommt, kann dies zu Risiken für die Persönlichkeitsrechte der Personen, deren Daten verarbeitet werden, führen. Die Gefahr eines Datenmissbrauchs oder einer unzulässigen Einflussnahme durch Dritte ist bei der Telearbeit oder dem Mobilen Arbeiten höher, da der Arbeitgeber/Dienstherr nur eingeschränkte Kontroll- und Einflussmöglichkeiten hat.

4 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/Dienstherrn gewährleistet ist.

5 Welche Daten sind besonders schützenswert?

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. Eine Verarbeitung dieser Daten ist untersagt, wenn keine Ausnahmen gemäß Art. 9 Abs. 2 und 3 DSGVO bestehen.

Beschäftigtendaten

Arbeitgeber/Dienstherren 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) – für Beamte sowie Beamtinnen und Tarifbeschäftigte in Verbindung mit §§ 106 ff. Bundesbeamtengesetz (BBG) – eines besonderen Schutzes und unterliegen oftmals dem Personalaktengeheimnis.

Sozialdaten

Als besonders schützenswert sind auch personenbezogene Daten anzusehen, welche die gesetzlichen Sozialversicherungsträger (dies sind beispielsweise Kranken- und Pflegekassen, Renten-, Unfallversicherungsträger, Bundesagentur für Arbeit, Jobcenter) 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 ihrer Sozialdaten.

Unterschiede auch bei besonders schützenswerten 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 besonders schützenswerten 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.

6 Risiken bei 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 oder unbefugten Zugriffs beim Umgang mit personenbezogenen Daten angesichts der gegebenen konkreten Arbeitsabläufe einzustufen ist.

Telearbeit und Mobiles Arbeiten sollten grundsätzlich als eine voll elektronische Datenverarbeitung ohne Medienbruch, also ohne Wechsel der Medien, ausgestaltet werden. Das heißt, die schriftliche Kommunikation mit dem Arbeitgeber/Dienstherrn, 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 Notwendigkeit Unterlagen zu transportieren, was ein hohes Risiko des Verlusts, der Beschädigung sowie der unbefugten Kenntnisnahme mit sich bringt.

Bei medienbruchfreier Gestaltung birgt Telearbeit ein geringeres Missbrauchsrisiko als das Mobile Arbeiten. Im Gegensatz zu Mobilem Arbeiten können 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. Das hierdurch gegebene Risiko eines unbefugten Zugriffs auf personenbezogene Daten durch unbefugte Dritte 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 vom 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-/behörden-interne Infrastruktur über ein sogenanntes Virtual Private Network (VPN) erfolgt, das die Verbindung zum firmen-/behörden-internen Netz durch eine ausreichend starke Verschlüsselung schützt.

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

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

7 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 (BSI) für das Mobile Arbeiten in der Bundesverwaltung zugelassen wurden. Dem Einsatz von durch den Arbeitgeber/Dienstherrn bereitgestellter IT-Ausstattung sollte der Vorzug vor der Nutzung privater Hard- und Software (Bring your own Device – BYOD) gegeben werden. Sollte es zu einer Verwendung privater Hard- und Software der Beschäftigten kommen, so sind Vereinbarungen

über die Kontrolle und Löschung beruflicher Daten sowie die deutliche Trennung von beruflichen und privaten Inhalten zu treffen. Neben dem Abschluss entsprechender Vereinbarungen ist die Trennung von beruflichen und privaten Inhalten auch technisch sicherzustellen. Darüber hinaus ist zu beachten, dass mit der dienstlichen Nutzung von für den privaten Gebrauch vorgesehener Software urheberrechtliche Fragestellungen verbunden sein können.

Das Risiko kann darüber hinaus minimiert werden, wenn durch den Arbeitgeber/Dienstherrn 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) 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,
- Vermeidung des Einsatzes von Smart Home-Geräten wie zum Beispiel smarten Lautsprechern oder digitalen Assistenten in den Räumen, in denen Telearbeit oder Mobiles Arbeiten stattfindet,
- hohe Sensibilität bei Telefonaten im privaten und öffentlichen Raum.

Weitere Hinweise zu datensicherem Mobilen Arbeiten finden sich in der Broschüre „Sicheres mobiles Arbeiten“ auf der Website des BSI, unter www.bsi.bund.de → Publikationen.

8 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.

9 Kontrollrechte und -pflichten

Da letztendlich die Arbeitgeber/Dienstherren 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 schützenswerte Daten während der Nutzung von Telearbeit oder Mobilem Arbeiten verarbeitet werden sollen.

Es muss durch geeignete technische und organisatorische Maßnahmen sichergestellt werden, dass der Arbeitgeber/Dienstherr eine datenschutzwidrige Nutzung des mobilen Gerätes entdecken kann, z. B. durch Protokollierung. Der Einsatz eines Mobile Device Managements wird empfohlen.

Im Rahmen von Telearbeit muss der Arbeitgeber/Dienstherr darüber hinaus die Möglichkeit des Zugangs zur Wohnung der 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 Beschäftigten 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 Arbeitgebers/Dienstherrn muss daher vertraglich mit den in Telearbeit Beschäftigten vereinbart werden, wobei auch das Einverständnis der in häuslicher Gemeinschaft mit ihnen zusammenlebenden Personen umfasst sein muss. Die sonstigen Kontrollberechtigten, wie z. B. die jeweiligen Beauftragten für den Datenschutz, sollten in das Zutrittsrecht einbezogen werden.

10 Weitere datenschutzrechtliche Empfehlungen

- Verantwortlichkeiten im Umgang mit personenbezogenen Daten sind umfassend vertraglich festzulegen.
- Grundsätzlich ist der Einsatz privater Hard- und Software für Telearbeit und das Mobile Arbeiten zu vermeiden. Erfolgt dennoch ein Einsatz privater Hard- und Software, so sind die vorstehenden Ausführungen zu BYOD und einem Mobile Device Management zu beachten.
- 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 Telearbeitenden in häuslicher Gemeinschaft lebenden Personen dürfen keinen Zugriff auf betriebliche/dienstliche Unterlagen haben. Die hierfür erforderlichen Sachmittel

sind vom Arbeitgeber/Dienstherrn 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 jeweilige betriebliche oder behördliche Datenschutzbeauftragte rechtzeitig zu beteiligen.
- → Bei der Einrichtung eines Telearbeitsplatzes soll der/die jeweilige betriebliche oder behördliche Datenschutzbeauftragte eingebunden werden. Er/Sie kann allgemeine oder konkrete Vorgaben machen. Dem/Der Datenschutzbeauftragten sind die erforderlichen Kontrollrechte einzurichten.
- → Während des Mobilen Arbeitens sind Sichtschutzfolien auf Displays zur Vermeidung unbefugter Kenntnisnahme von personenbezogenen Daten zu verwenden.

Informationen rund um das Thema
„Arbeit und Bildung“
finden Sie auf www.bfdi.bund.de.

Herausgegeben von

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Postfach 14 68
53004 Bonn
Tel. +49 (0) 228 99 77 99-0
Fax +49 (0) 228 99 77 99-5550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH

Bildnachweis: Getty Images International

Stand: Juli 2020