



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



Telearbeit

Ein Datenschutz-Wegweiser





Inhalt

Was ist Telearbeit?	4
Ist Telearbeit mit dem Datenschutz vereinbar?	5
Vorsicht bei besonders sensiblen Daten!	6
Welche Daten sind besonders schutzwürdig?	6
Unterschiede auch bei schutzwürdigen Daten	7
Risiken bei den Arbeitsabläufen	8
Datensicherheit beim IT-Einsatz	10
Sicherer Transport von Unterlagen und Datenträgern	11
Kontrollrecht und -pflichten	12
Weitere datenschutzrechtliche Empfehlungen	14

Was ist Telearbeit?

Als Telearbeit gelten Arbeitsformen, bei denen Beschäftigte zumindest einen Teil ihrer Aufgaben nicht an dem von ihrem Arbeitgeber zur Verfügung gestellten Arbeitsplatz verrichten, sondern an anderer Stelle, in den meisten Fällen in ihrer eigenen Wohnung. Nicht unter den Begriff Telearbeit fallen Tätigkeiten, die wegen der besonderen Art ihrer Ausübung an keinem festen Arbeitsplatz erledigt werden (z. B. Handelsvertreter). Vor dem Hintergrund einer fortschrittlichen Familien- und Gleichstellungspolitik und der zunehmenden Flexibilisierung von Arbeit spielt Telearbeit eine immer größere Rolle. So wurde bereits im Jahr 2002 von den europäischen Sozialpartnern eine Rahmenvereinbarung Telearbeit entwickelt, die in den Mitgliedstaaten von den Sozialpartnern in die Praxis umgesetzt werden soll. Im Jahr 2006 haben die Sozialpartner einen Bericht über die Umsetzung vorgelegt. Mit Ausnahme der Slowakei, Zyperns, Estlands und Litauens haben die Mitgliedstaaten danach die Rahmenvereinbarung tatsächlich umgesetzt.



Ist Telearbeit mit dem Datenschutz vereinbar?

Ob Telearbeit bei bestimmten beruflichen Tätigkeiten aus datenschutzrechtlichen Gründen unzulässig ist, ist gesetzlich nicht klar geregelt. Werden an einem Telearbeitsplatz nur Daten ohne Personenbezug verarbeitet, ist dies datenschutzrechtlich uneingeschränkt möglich.

Die Verlagerung von Tätigkeiten in den häuslichen Bereich, bei denen personenbezogene Daten verarbeitet werden, birgt allerdings Risiken für die Persönlichkeitsrechte der Betroffenen, da Datenmissbrauch oder eine unzulässige Einflussnahme durch Dritte – auch wegen den eingeschränkten Kontroll- und Einflussmöglichkeiten des Arbeitgebers – leichter möglich ist. Aber auch hier schließt Datenschutz Telearbeit nicht grundsätzlich aus. Es sollte jedoch in jedem Einzelfall vorher unter Berücksichtigung der Art der zu verarbeitenden Daten und ihres Verwendungszusammenhangs sorgfältig und differenziert geprüft werden, ob die Wahrnehmung der jeweiligen Aufgaben oder Tätigkeiten in Telearbeit datenschutzrechtlich vertretbar oder hiervon abzuraten ist. Die Entscheidung muss der Arbeitgeber eigenverantwortlich selbst treffen.

Dabei spielen u. a. folgende Gesichtspunkte eine Rolle:

Vorsicht bei besonders sensiblen Daten!

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

Welche Daten sind besonders schutzwürdig?



■ Beschäftigtendaten

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

■ Sozialdaten nach § 67 Sozialgesetzbuch X (SGB X)

Als äußerst schutzwürdig sind auch personenbezogene Daten anzusehen, die die gesetzlichen Sozialversicherungsträger (Kranken- und Pflegekassen, Renten-, Unfallversicherungsträger, Bundesagentur für Arbeit, Jobcenter) zur Aufgabenerfüllung über ihre Mitglieder bzw. Versicherten speichern. Diese Sozialdaten unterliegen dem Sozialgeheimnis, das die Verpflichtung umfasst, sicherzustellen, dass die Daten nur Befugten zugänglich sind und nur an diese weitergegeben werden.

■ Angaben nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG)

Zu den besonders sensiblen personenbezogenen Daten gehören vor allem die in § 3 Abs. 9 BDSG genannten Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben einzelner Personen.

Unterschiede auch bei schutzwürdigen Daten

Bei der Entscheidung, ob und ggf. unter welchen Vorkehrungen sich bestimmte Aufgaben für Telearbeit eignen, gilt es jedoch auch hinsichtlich des Umgangs mit besonders sensiblen personenbezogenen Daten zu differenzieren.



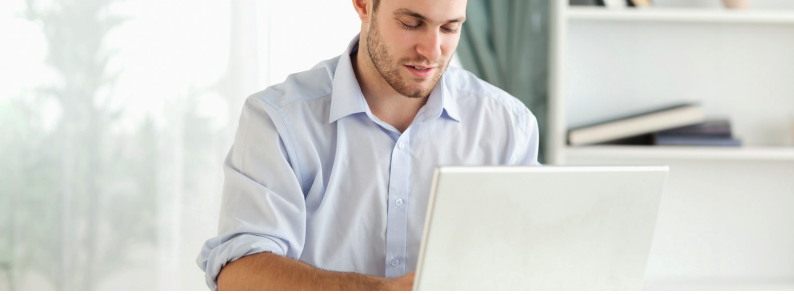
Grundsatz: Je sensibler und damit schützenswerter personenbezogene Daten sind, desto stärker sind sie zu schützen.

So können z. B. im Bereich der Beschäftigtendaten personenbezogene Informationen über Aus- und Fortbildung durchaus geeignet sein, im Rahmen von Telearbeit verarbeitet zu werden. Voraussetzung ist auch hier, dass – ebenso wie z. B. an einzelnen Telearbeitsplätzen, an denen Sozialdaten verarbeitet werden sollen – ausreichende technische und organisatorische Maßnahmen zum Schutz dieser sensiblen Daten umgesetzt sind. Hierbei ist auch das jeweilige Datenschutz- bzw. Datensicherheitskonzept des Arbeitgebers von Bedeutung.

Daten über Beurteilungen oder Erkrankungen eignen sich dagegen generell nicht zur häuslichen Verarbeitung. Hier wäre das unvermeidbare Restrisiko für einen Datenmissbrauch nicht hinnehmbar.

Risiken bei den Arbeitsabläufen

Für die Bewertung, ob und ggf. unter welchen Umständen für eine bestimmte Tätigkeit Telearbeit in Betracht kommt, spielt auch eine Rolle, wie hoch das Risiko eines Missbrauchs im Umgang mit personenbezogenen Daten bei den konkreten Arbeitsabläufen ist.



Bei der Telearbeit finden in der heutigen Zeit die Kommunikation mit dem Arbeitgeber, die Entgegennahme von Aufgaben, der Umgang mit personenbezogenen Daten und die Übermittlung der Arbeitsergebnisse in aller Regel automatisiert mit Hilfe von IT-Einrichtungen und über elektronische Kommunikationswege statt.

Eine solche voll elektronische Datenverarbeitung ohne Medienbruch ist anders zu beurteilen als die konventionelle Verarbeitung, bei der Unterlagen oder Akten zwischen Büro des Arbeitgebers und Telearbeitsplatz hin und her transportiert werden müssen. In letzterem Fall ist das Risiko des Verlusts, der Beschädigung sowie der unbefugten Kenntnisnahme ungleich höher. Dies gilt einerseits für den Transportweg, andererseits aber auch am Telearbeitsplatz des Arbeitnehmers selbst, wo ein Betreten des Arbeitszimmers durch Dritte nicht gleichermaßen sicher unterbunden werden kann, wie in den Räumen des Arbeitgebers. Sind also im Rahmen einer konventionellen Verarbeitung besonders schutzbedürftige Daten betroffen, sollte von der Wahrnehmung der Tätigkeit in Telearbeit abgesehen werden.

Bei einer Datenverarbeitung im Auftrag (§ 11 BDSG; § 80 SGB X) sollte Telearbeit beim Auftragnehmer grundsätzlich nicht zugelassen werden. Das Sicherheitsrisiko ist bei dieser Art der Datenverarbeitung sehr hoch und die Kontrollmöglichkeiten der verantwortlichen Stelle sind sehr eingeschränkt.

Datensicherheit beim IT-Einsatz

Bei einer voll elektronischen Datenübermittlung sind Maßnahmen zur Sicherung der Vertraulichkeit und Authentifizierung der Kommunikationspartner nach dem Stand der Technik (Verschlüsselungsverfahren etc.) erforderlich.

Das Risiko kann darüber hinaus minimiert werden, wenn durch den Arbeitgeber im Rahmen der erforderlichen technisch-organisatorischen Maßnahmen (§ 9 BDSG und die Anlage hierzu) zumindest die folgenden Vorgaben erfüllt sind:

- Separates, abschließbares Arbeitszimmer,
- Trennung zwischen beruflichem und privaten (Internet-)Anschluss,
- Zugang des Berechtigten zu den sensiblen personenbezogenen Daten nur mit Benutzer-ID und PIN oder Karte (Einsatz zertifizierter Kartenlesegeräte erforderlich),
- Verbindung ausschließlich über ein sogenanntes Virtual Private Network (VPN),
- Verschlüsselung der Daten (Ende-zu-Ende-Sicherheit),
- Zugangsmöglichkeit des Arbeitgebers und dessen Beauftragten für den Datenschutz sowie der zuständigen Datenschutzaufsichtsbehörde zum Telearbeitsplatz und dessen IT-Einrichtungen zu Kontrollzwecken unter Berücksichtigung des Art. 13 GG (s. dazu sogleich),
- Sperrung von USB-Zugängen und anderen Anschlüssen,

- falls erforderlich, sichere Anbindung eines lokalen Druckers (kein Netzwerkdrucker, kein WLAN-Drucker, kein online-Drucker!!!) in unmittelbarer Nähe des Arbeitsplatzes mit Protokollierung von häuslichen Druckvorgängen,
- keine private Nutzung der beruflich zur Verfügung gestellten IT-Ausstattung.



Sicherer Transport von Unterlagen und Datenträgern

Müssen bei der Telearbeit Unterlagen oder Datenträger (CDs, USB-Sticks etc.) von den Beschäftigten zwischen Telearbeitsplatz und Büro beim Arbeitgeber hin und her 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

Nicht zuletzt wegen der letztendlich vom Arbeitgeber/Dienstherr zu verantworteten Risiken genügt es nicht, technisch-organisatorische Vorgaben zu treffen. Vielmehr hat der Arbeitgeber/Dienstherrn nicht nur das Recht, sondern auch die Pflicht, vor und nach der Genehmigung der Telearbeit routinemäßig und in regelmäßigen Abständen zu kontrollieren, dass diese Vorgaben auch eingehalten werden. Dies gilt insbesondere, soweit besonders sensible Daten (Sozialdaten, Daten i.S.v. § 3 Abs. 9 BDSG) durch Telearbeit verarbeitet werden sollen. Um seinen Kontrollpflichten gerecht zu werden, muss der Arbeitgeber die Möglichkeit des Zugangs zur Wohnung des Telearbeiters haben (s. o.). Art. 13 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 dem Arbeitnehmer 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 muss daher vertraglich mit dem Telearbeiter vereinbart werden. Die sonstigen Kontrollberechtigten, wie z. B. der betriebliche oder der behördliche Beauftragte für den Datenschutz, sollten in das



Zutrittsrecht einbezogen werden. Da der Arbeitgeber auch die Möglichkeit der staatlichen Kontrolle (durch den BfDI oder die Aufsichtsbehörden nach § 38 BDSG) sicherzustellen hat, die staatlichen Stellen jedoch aufgrund des Art. 13 GG, der diese unmittelbar verpflichtet, keinen Zugang zu Privatwohnungen haben, sollte durch entsprechende Vereinbarung mit dem Beschäftigten auch die Kontrollmöglichkeit durch die Aufsichtsbehörden sichergestellt werden. Wichtig ist darüber hinaus, dass auch die Zustimmung der Personen, die mit dem Telearbeitnehmer in häuslicher Gemeinschaft leben, eingeholt wird.

Weitere datenschutz- rechtliche 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 darf am Telearbeitsplatz nicht eingesetzt werden;
- Berufliche E-Mails und Telefonate dürfen nicht auf private Postfächer oder private Telefonanschlüsse/ Handys der Telearbeiter umgeleitet werden;
- Es müssen geeignete häusliche Räumlichkeiten und Arbeitsmittel zur sicheren Aufbewahrung und vertraulichen Behandlung von Unterlagen und Datenträgern mit personenbezogenen Daten vorhanden sein. Auch die mit dem Telearbeiter in häuslicher Gemeinschaft lebenden Personen dürfen keinen Zugriff auf dienstliche Unterlagen haben. Die hierfür erforderlichen Sachmittel, z. B. verschließbare Einrichtungsgegenstände, sind vom Arbeitgeber zur Verfügung zu stellen. Dies sollte auch die Möglichkeit beinhalten, Daten vor Ort datenschutzgerecht vernichten zu können;
- Bei der Entscheidung über einen Telearbeitsplatz ist der Beauftragte für den Datenschutz des Arbeitgebers rechtzeitig zu beteiligen;

- Die Datenschutzgrundsätze für Telearbeit sind in einer Betriebs-/Dienstvereinbarung festzuschreiben.
- Bei der Einrichtung eines Telearbeitsplatzes soll der/die behördliche oder betriebliche Datenschutzbeauftragte (bDSB) eingebunden werden. Er/Sie können allgemeine oder konkrete Vorgaben machen. Dem/Der bDSB sind die erforderlichen Kontrollrechte einzurichten.

Weitere Informationen finden Sie auf der Homepage des BfDI unter dem Stichwort „Telearbeit“.



Herausgeber:

Die 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 99-550
E-Mail: referat12@bfdi.bund.de
Internet: www.datenschutz.bund.de

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

Stand: Mai 2016

Dieser Flyer ist Teil der Öffentlichkeitsarbeit der BfDI. Er wird
kostenlos abgegeben und ist nicht für den Verkauf bestimmt.