



Der 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	9
Sicherer Transport von Unterlagen und Datenträgern	10
Weitere datenschutzrechtliche Empfehlungen	11



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 mittels elektronischer Kommunikation an anderer Stelle, in den meisten Fällen in ihrer eigenen Wohnung.



Ist Telearbeit mit dem Datenschutz vereinbar?

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

Die Verlagerung von Tätigkeiten in den häuslichen Bereich, bei denen personenbezogene Daten verarbeitet werden, birgt allerdings Risiken für die Persönlichkeitsrechte der Betroffenen, weil ein Datenmissbrauch leichter möglich ist. Es sollte daher in jedem Einzelfall vorher geprüft werden, ob die Wahrnehmung solcher Aufgaben in Telearbeit datenschutzrechtlich vertretbar ist. Die Entscheidung muss der Arbeitgeber eigenverantwortlich selbst treffen.

Dabei spielen 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 entsprechenden Kontrollmöglichkeiten des Arbeitgebers vor Ort gewährleistet ist.



■ Sozialdaten nach § 67 SGB X

Dies sind personenbezogene Daten, die die gesetzlichen Sozialversicherungsträger (Kranken- und Pflegekassen, Renten-, Unfallversicherungsträger, Bundesagentur für Arbeit, Jobcenter) über ihre Mitglieder bzw. Versicherten speichern.

■ Angaben nach § 3 Abs. 9 BDSG

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

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 und oftmals dem Personalakte geheimnis unterliegen.



Unterschiede auch bei schutzwürdigen Daten

Bei der Entscheidung, ob und ggf. unter welchen Vorkehrungen sich bestimmte Aufgaben für Telearbeit eignen, gilt es jedoch 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 ausreichende technische und organisatorische Maßnahmen zum Schutz dieser sensiblen Daten umgesetzt sind.

Daten über Beurteilungen oder Erkrankungen eignen sich dagegen generell nicht zur häuslichen Verarbeitung.

Auftragnehmer grundsätzlich nicht zugelassen werden. Das Sicherheitsrisiko ist bei dieser Art der Datenverarbeitung sehr hoch und die Kontrollmöglichkeiten der verantwortlichen Stelle sind sehr eingeschränkt.



Risiken bei den Arbeitsabläufen

Für die Bewertung spielt auch eine Rolle, wie hoch das Risiko eines Missbrauchs bei den konkreten Arbeitsabläufen ist.

So ist die vollelektronische Datenverarbeitung ohne Medienbruch anders zu beurteilen als die konventionelle Bearbeitung, bei der Unterlagen zwischen Büro des Arbeitgebers und Telearbeitsplatz hin und her transportiert werden müssen.

Bei einer Datenverarbeitung im Auftrag (§ 11 BDSG; § 80 SGB X) sollte Telearbeit beim

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 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 privatem (Internet-)Anschluss,
- Zugang des Berechtigten zu den sensiblen personenbezogenen Daten nur mit Benutzer-ID und PIN oder Karte (Einsatz zertifizierter Kartenlesegeräte erforderlich),
- Verbindung 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,
- Sperrung von USB-Zugängen und anderen Anschlüssen,
- Falls erforderlich, sichere Anbindung eines lokalen Druckers 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

Beim Transport von Unterlagen oder Datenträgern zwischen Telearbeitsplatz und Büro sind folgende Mindestanforderungen zu gewährleisten:

- Datenträger nur verschlüsselt und Papierunterlagen nur in verschlossenen Behältnissen transportieren,
- Datenträger und Unterlagen nie unbeaufsichtigt lassen.

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 darf am Telearbeitsplatz nicht eingesetzt werden;
- Berufliche E-Mails und Telefonate dürfen nicht auf private Postfächer oder private Telefonanschlüsse/Handys der Telearbeiter umgeleitet werden;
- Bei der Entscheidung über einen Telearbeitsplatz ist der Beauftragte für den Datenschutz des Arbeitgebers rechtzeitig zu beteiligen;
- Die Datenschutzgrundsätze für Telearbeit sollten in einer Betriebs-/Dienstvereinbarung festgeschrieben werden.

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



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 99-550
E-Mail: ref3@bfdi.bund.de
Internet: www.datenschutz.bund.de

Realisation: Diamond media GmbH
Bildnachweis: dreamstime, fotolia, iStockphoto

Stand: August 2012