DSGVO

Tipps zu speziellen Bereichen der Telearbeit

von RA Heike Mareck, externe Datenschutzbeauftragte, Dortmund

| Telearbeit bzw. Homeoffice funktioniert, das hat bereits die Vergangenheit gezeigt. Doch was muss der Arbeitgeber beachten, wenn er für die Zukunft den Homeoffice-Bereich seiner Arbeitnehmer datenschutzkonform einrichten will? Nachfolgend einige Tipps zu den Bereichen rund um Datenspeicherung, Privatnutzung und Sicherheitsniveau. |

Keine Frage: Der Arbeitnehmer greift auf die personenbezogenen Daten (Kunden-, Lieferanten-, Subunternehmerdaten) des Arbeitgebers zurück, wenn er von zu Hause aus arbeitet. Der Arbeitgeber muss daher auch in diesem Fall sicherstellen, dass die Voraussetzungen nach Art. 32 ff. DSGVO (Sicherheit personenbezogener Daten) eingehalten bzw. erfüllt werden. Denn er bleibt nach Art. 4 Nr. 7 DSGVO „Verantwortlicher“ für die Datenverarbeitung.

Eins vorweg: Die Tipps sind insbesondere für die Fälle der Einsätze im Homeoffice und im Mobiloffice gedacht. Das heißt, die IT-Ausrüstung stellt der Arbeitgeber. Sollte der Arbeitnehmer seinen eigenen Computer, sein Tablet, Handy oder Drucker einsetzen müssen, gilt das Prinzip „Bring Your Own Device“, so nennt man es, wenn Mitarbeiter ihr privates Handy oder Notebook im Job nutzen. „Bring Your Own Device“ birgt enorme Risiken für den Arbeitgeber. Dieser ist verantwortlich für den Schutz der Daten, mit denen die Firma arbeitet. Daran ändert sich auch nichts, wenn der Arbeitnehmer für die Arbeit eigene Geräte nutzt.

Anforderungen an die Datenspeicherung

Gehen wir im Weiteren davon aus, dass die IT-Ausrüstung durch den Arbeitgeber gestellt wird. Zunächst ist wichtig, dass die Tätigkeit im Rahmen des Homeoffices auch im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO ihren Niederschlag findet. Auskunftsersuchen Dritter können für den Arbeitgeber mit Schwierigkeiten verbunden sein, weil letztlich jeder Rechner in jedem Homeoffice zur Auskunftserteilung durchsucht werden muss. Der Arbeitgeber muss daher seine EDV so gestalten, dass er seinen Auskunftspflichten in der gebotenen Schnelligkeit und mit betrieblich vertretbarem Aufwand nachkommen kann.

Um den IT-Sicherheitsanforderungen zu entsprechen, sollten die Daten zentral auf den Servern des Arbeitgebers gespeichert sein und der Arbeitnehmer sich diese etwa per Terminal-Zugriff anzeigen lassen.

Daten sollten nur in Ausnahmefällen lokal gespeichert werden. Die lokale Speicherung ist im Idealfall nicht nur im Verzeichnis der Verarbeitungstätigkeiten erwähnt. Ein verantwortungsvoller Umgang mit Daten zeichnet sich dadurch aus, dass im Unternehmen Richtlinien über Auskunftsersuchen Betroffener bestehen, die belegen, welche Arten oder Gruppen von Daten der lokalen Speicherung unterfallen.

Nach Art. 12 Abs. 3 DSGVO ist die Auskunft durch den Verantwortlichen unverzüglich, also ohne schuldhaftes Zögern, zu erteilen. Darüber hinaus gilt eine Obergrenze von einem Monat. Die darf nur überschritten werden, wenn die konkrete Anfrage besonders komplex ist. Auch muss die konkrete, zum Zeitpunkt der Fristverlängerung vorliegende Anzahl der Anfragen das übliche Maß deutlich überschreiten. Verspätete, falsche, unvollständige oder gar nicht erteilte Auskünfte können mit einer Geldbuße belegt werden. Auch andere Maßnahmen, wie die Versicherung der Richtigkeit und Vollständigkeit an Eides statt analog §§ 259, 260 BGB oder eine Strafbarkeit bei falscher oder unvollständiger Auskunftserteilung drohen.

Lokal gespeicherte Daten stellen besondere Anforderungen an die technisch-organisatorischen Maßnahmen (TOMs) nach Art. 32 DSGVO. Oft ist schon die Zutrittskontrolle mit Schwierigkeiten verbunden, da die Arbeitnehmer, die die Telearbeit ausführen, mit anderen Mitbewohnern oder Lebenspartnern zusammenwohnen bzw. auch die Wohnungen/Häuser nicht auf Unternehmensniveau gesichert sind. Hier ist eine Festplattenverschlüsselung eine gute Alternative. Einige Computer, vor allem Notebook-Modelle für Geschäftskunden, sind mit einem Trusted Platform Module (TPM) ausgestattet. Empfehlungen zur hardwareunterstützten Verschlüsselung für PCs und Notebooks, Festplatten, externe Festplatten und Speichersticks, sowie Netzwerkspeicher (NAS) finden Sie unter www.iww.de/s2555.

Datensicherung bedeutet auch, dass die Speicherung bzw. Spiegelung der Daten zusätzlich außerhalb der Wohnung erfolgen sollte. Hierbei sollte man sich stets die Frage stellen: Was passiert, wenn die Wohnung abbrennt? Wo liegen dann noch die Daten? Die Erlaubnis zu lokaler Datenspeicherung sollte

- schriftlich erfolgen und
- konkret formuliert werden.

PRAXISTIPP | Es sollte ausdrücklich geregelt werden, dass es verboten ist, betriebliche Daten auf anderen Speichermedien als vom Arbeitgeber schriftlich zugelassen zu speichern.

Eine zusätzliche Formulierung kann lauten: Erlaubt ist die Speicherung auf folgenden betrieblichen Servern (Laufwerk […])...

Regeln Sie zusätzlich, was auch verboten sein soll. Zum Beispiel: Die Speicherung von betrieblichen Daten ist insbesondere auf privaten Smartphones, USB-Sticks, Computern o. Ä. verboten.

Privatnutzung der Ausrüstung des Arbeitgebers

Es besteht im Rahmen der Telearbeit im Gegensatz zur Tätigkeit beim Arbeitgeber kein Grund, die private Internetnutzung zu gestatten. Denn alle Arbeitnehmer verfügen zu Hause über einen eigenen Internetzugang. Darüber hinaus muss der Arbeitgeber auch für das Homeoffice die Datensicherheit gewährleisten und effektive Kontrollen vornehmen können. Dies wird bei einer auch nur eingeschränkten privaten Nutzungsmöglichkeit des vom Arbeitgeber gestellten Equipments für die Telearbeit unnötig

erschwert. Auch die Risiken der Störerhaftung und der Inanspruchnahme des Arbeitgebers bei Urheberrechtsverletzungen sollten insofern im Auge behalten werden.

PRAXISTIPP | Es sollte klar geregelt sein, dass die private Nutzung der für den Heimarbeitsplatz bereitgestellten betrieblichen Geräte bzw. Zugangsmöglichkeiten (insbesondere Computer und Internetzugang) verboten ist.

Praktische Fragen zum Sicherheitsniveau

Immer wieder gibt es Probleme, wenn der Arbeitnehmer die Unterlagen „offen" liegen lässt – nicht nur während einer kurzen Abwesenheit, sondern auch zum Beispiel im Urlaub, oder wenn Mitbewohner die Unterlagen einsehen können. Es sollte deutlich geregelt werden, dass auch das Sicherheitsniveau der zur Verfügung gestellten Hard- und Software i. S. v. Art. 32 DSGVO eingehalten wird.

Checkliste / Datenschutz bei Telearbeit

- Der Arbeitnehmer sollte im Homeoffice statt mit Klardaten besser mit Pseudonymen – z. B. Aktenzeichen – umgehen. Beim Einsatz von Papierakten ist besondere Vorsicht geboten: Denn diese enthalten meist Klarnamen und können nicht pseudonymisiert werden. Zudem ist bereits der Transport vom Arbeitgeber zum Einsatz beim Arbeitnehmer und wieder zurück ein Sicherheitsrisiko. Hier ist der Arbeitgeber angehalten, besondere Sicherheitsmaßnahmen zu treffen.

- Um Datendiebstahl des Arbeitnehmers zu vermeiden, ist eine schriftliche Dokumentation zu empfehlen. Das heißt, der Vorgesetzte sollte stets abzeichnen, welche Akten der im Homeoffice tätige Arbeitnehmer „mitnimmt", um zu wissen, woran er arbeitet und welche Akte gerade „aushäusig" ist. Dies ist ein nicht unerheblicher Verwaltungsvorgang.

- Erfolgt die Mitnahme der „Akten" durch mobile Speichermedien, sollten diese stets verschlüsselt sein.

- Es sollte explizit geregelt werden, dass und nach welcher Zeit der Arbeitsunterbrechung sich der Computer automatisch sperrt bzw. ob eine automatische Abwesenheitserkennung eingesetzt werden kann.

- Kann nicht ausgeschlossen werden, dass ein Dritter auf den Computer Zugriff hat, sollten die Mitarbeiter zur manuellen Sperrung verpflichtet werden.

- Wer als Arbeitnehmer den Drucker nutzt, um Unterlagen für die Akte auszudrucken, benötigt in jedem Fall einen datenschutzkonformen Aktenvernichter.