DATENSCHUTZ IM HOME-OFFICE

EIN ÜBERBLICK

Im Zuge unserer Home-Office-Inforeihe, ist das Thema des Umgangs mit Daten gerade auch bei kleinen und mittleren Unternehmen ein Bereich, über den hier informiert werden soll, der aber rechtlich von jedem Unternehmen selbst zu prüfen ist. Die Vereinbarkeit von Beruf und Familie innerhalb der familienbewussten Personalpolitik bedeutet auch, dass sich die Fachkräfte im Home-Office gerade bei diesem Thema in einem abgesicherten Bereich befinden.

Der Datenschutz schließt Telearbeit und Arbeiten nicht grundsätzlich aus. Es sollte dabei 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.

FOLGENDE FAKTOREN SOLLTEN UNBEDINGT GEPRÜFT WERDEN

Werden personenbezogene oder Sozialdaten verarbeitet, die in besonderer Weise schützenswert und sensibel handzuhaben sind? Dies sollte vom Datenschutzbeauftragten oder passender Rechtsstelle geprüft und dementsprechend eingestuft werden. Nur so ist ein Datenschutzkonformer Umgang durch die Angestellten mit den Daten möglich. Außerdem bedarf es in solchen Fällen besonderer Sicherheitsmaßnahmen hinsichtlich Hard- und Software.

SICH DARAUS ERGEBENDE MAßNAHMEN AM HEIMARBEITSPLATZ

Im Home-Office trägt der Arbeitgeber die datenschutzrechtliche Verantwortung. Daher sollte auf folgende Punkte geachtet werden, wobei gilt, je sensibler und schützenswerter die personenbezogenen Daten sind, umso stärker muss der Schutz sein:

- das Arbeitszimmer sollte separat und abschließbar sein
- dienstliche Unterlagen sollten in einem abschließbaren Schrank aufbewahrt werden
- die beruflich zur Verfügung gestellte IT-Ausstattung sollte nicht privat genutzt werden
- die Festplatte des PCs / Laptops sollte verschlüsselt werden, ebenso externe Datenträger wie USB-Sticks
- das Betriebssystem ist mit einem Kennwort zu versehen

Stand: März 2020

Das Kompetenzzentrum Frau und Beruf Bonn/Rhein-Sieg wird gefördert von:
Ministerium für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen
EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung

Träger:
ZUKUNFT. FUTURE. AVENIR. BONN.
:rhein-sieg-kreis

- die elektronische Datenübermittlung (also z.B. E-Mail) ist nach dem Stand der Technik zu verschlüsseln
- wenn der Ehegatte/ Kinder oder Dritte (beispielsweise in einer Wohngemeinschaft) mit unter einem Dach wohnen, sollte der Computer auch bei kurzzeitigem Verlassen gesperrt werden
- berufliche E-Mails sind nicht auf private E-Mail-Postfächer weiterzuleiten
- Konzept zum Umgang und Vernichtung von sensiblen Unterlagen und Ausdrucken

Im Einzelfall kann es erforderlich sein, dass der Arbeitgeber und der zuständigen Datenschutzbehörde zu Kontrollzwecken eine Zugangsmöglichkeit hat.
Bei der Planung sollten Datenschutzbeauftragte frühzeitig beteiligt werden. Zum einen zur Frage, ob und in welchem Umfang Home-Office bei Mitarbeitern datenschutzrechtlich in Betracht kommt und zum anderen, welche Schutzmaßnahmen im Einzelnen zu treffen sind.

BESONDERHEITEN BEI MOBILEM ARBEITEN

Mobiles Arbeiten birgt Risiken, wie zum Beispiel Geräteverlust, arbeiten an öffentlichen Plätzen und Einsicht durch Dritte oder auch unsichere Datenübertragung. Dieses Risiko kann allerdings reduziert werden:

- Die Daten auf dem mobilen Gerät müssen verschlüsselt werden
- Der Transport des mobilen Gerätes sollte 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) sollten über mobile Geräte nur genutzt werden, wenn ein Zugriff auf die firmeninterne Infrastruktur über ein sogenanntes Virtual Private Network (VPN) erfolgt, das die Verbindung zum firmeninterne Netz durch eine ausreichend starke Verschlüsselung schützt.
- Es soll darauf geachtet werden, dass der Bildschirm und die Tastatur der genutzten mobilen Geräte durch Passanten und Videokameras nicht einzusehen sind.
- Dienstliche Telefonate mit Personenbezug sollten im öffentlichen Raum nur geführt werden, wenn ein Mithören ausgeschlossen werden kann.

DATENSCHUTZKONFORME MOBILGERÄTE

Um mobiles Arbeiten und Teleheimarbeit (Unterschiede siehe Inforeihe“ Formen der Telearbeit“) – soweit dabei mobile Geräte genutzt werden – datensicher zu gestalten, empfiehlt der BfDI (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) nur Geräte einzusetzen, die 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).

Stand: März 2020

Das Kompetenzzentrum Frau und Beruf Bonn/Rhein-Sieg wird gefördert von:
Ministerium für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen
EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung
Träger:
ZUKUNFT. FUTURE. AVENIR. BONN.
:rhein-sieg-kreis

- 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

INFORMATIONSPFLICHT BEI UNRECHTMÄßIGER KENNTNISERLANGUNG VON DATEN

Bei der Verarbeitung von besonderen personenbezogenen Daten ist bei der Einrichtung des Heimarbeitsplatzes stets an die Rechtsfolgen, die durch einen Verlust von Daten ausgelöst werden können und u.a. zu einer Informationspflicht gegenüber der zuständigen Aufsichtsbehörde führen können zu denken. (§ 42 a BDSG)

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.

Quellen:

https://www.datenschutzbeauftragter-info.de/home-office-datenschutz-bei-der-arbeit-von-zuhause/

Und PDF des BfDs „Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser“:
http://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.pdf?__blob=publicationFile

https://www.e-recht24.de/artikel/arbeitsrecht/11972-corona-home-office-datenschutz-arbeitsrecht.html

Das Kompetenzzentrum Frau & Beruf Bonn/Rhein-Sieg wünscht Ihnen viel Erfolg bei der Umsetzung und steht für weitergehende Informationen gerne zur Verfügung: info@kompetenzzentrum-frau-beruf.de

Weitere Informationen erhalten Sie unter www.familienbewussteUnternehmen.de Oder unter www.competentia.nrw.de/bonn_rhein-sieg.de

Stand: März 2020

Das Kompetenzzentrum Frau und Beruf Bonn/Rhein-Sieg wird gefördert von:
Ministerium für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen
EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung
Träger:
ZUKUNFT. FUTURE. AVENIR. BONN.
:rhein-sieg-kreis