Tipps für Remotearbeit

Im Rahmen der Digitalisierung und des Wunschs nach einer ausgeglichenen Work-Life-Balance gewinnt Homeoffice/ Telearbeit/ Remotearbeit zunehmend an Bedeutung. Neben der reinen technischen Umsetzung und der Befähigung der Mitarbeiter steht immer die Frage, welche Anforderungen dazu aus Datenschutzsicht bestehen. Zum Schutz der personenbezogenen Daten sind durch Unternehmen, Institutionen und Behörden passgenaue technische und organisatorische Maßnahmen aufzustellen, um Vertraulichkeit, Zweckbindung, Integrität und Verfügbarkeit zu garantieren. Daneben sollen auch Geschäftsgeheimnisse und Unternehmensinterna angemessen geschützt werden. Aus den zu treffenden Maßnahmen lassen sich einige Grundsätze ableiten. Arbeitgebern empfehlen wir, folgende Hinweise bei der Einführung von Remotearbeit zu berücksichtigen:

- Sensibilisieren Sie Ihre Mitarbeiter im Umgang mit personen- und unternehmensbezogenen Daten. Halten Sie bei Bedarf ein Konzept mit den Rahmenbedingungen bereit.
- Lassen Sie sich die Bekanntgabe und Verpflichtung zur Einhaltung dieser Regelungen durch Ihre Beschäftigten bestätigen. Vergessen Sie nicht die Einbindung des Betriebsrates/ Personalrates!
- Ist das Unternehmen als Auftragsverarbeiter tätig, klären Sie, inwieweit bei Tätigkeiten aus dem Homeoffice Anpassungen an die Vereinbarungen zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO erforderlich sind.
- Benennen Sie unter Ziffer 10 (siehe Seite 2) den Ansprechpartner und die Funktionsadresse für Rückfragen.

Ergänzende Informationen insbesondere zu befristeten tolerierten Abweichungen bei erforderlichen Schutzmaßnahmen durch Datenschutzaufsichtsbehörden während der Corona-Krise finden Sie z. B. über diese weiterführenden Links:

- „Informationen zum mobilen Arbeiten durch öffentliche Stellen“, Die Landesbeauftragte für den Datenschutz Niedersachsen, Abrufdatum 13. Mai 2020, https://lfd.niedersachsen.de/startseite/allgemein/mobiles-arbeiten-corona-186918.html
- „Corona-Pandemie – Hinweise des BayLDA zu Datenschutz und Datensicherheit, Bayerisches Landesamt für Datenschutzaufsicht, Abrufdatum 13. Mai 2020, https://www.lda.bayern.de/de/corona_datenschutz.html

Um Arbeitnehmern den Einstieg in die Remotearbeit zu erleichtern, hat der AWV-Arbeitskreis ‚Weiterentwicklung des Datenschutzrechts' zehn Tipps zusammengestellt:

1. Verwenden Sie nur die vom Arbeitgeber zur Verfügung gestellten technischen Lösungen und Emailadressen. Dazu zählen z. B. auch sogenannte Bootstick-Lösungen[1], bei der die private Hardware nur als technische Brücke zum Firmennetz dient und auf den privaten Geräten selbst keine Daten gespeichert werden.

2. Bewahren Sie die technischen Zugangsgeräte bei einer Zwei-Faktor-Authentifizierung[2] getrennt voneinander auf.

3. Geben Sie überlassene Hardware nicht zur Nutzung an Unberechtigte weiter und nutzen Sie diese Hardware nicht für private Zwecke.

4. Achten Sie darauf, dass Unberechtigte (z.B. Familienangehörige, Mitbewohner oder Nachbarn) nicht auf Ihren Bildschirm sehen können. Arbeiten Sie, sofern möglich, in einem separaten und abschließbaren Arbeitszimmer.

5. Sperren Sie bei Verlassen Ihres Arbeitsplatzes den Bildschirm Ihrer Endgeräte (z.B. Drücken der Tasten „Windows" und „L").

6. Stellen Sie sicher, dass das Mithören von dienstlichen Telefonaten und Onlinekonferenzen durch Unberechtigte nicht möglich ist. Denken Sie dabei daran, dass auch private Sprachassistenten „zuhören" und Gesprächsdaten speichern können. Auf der sicheren Seite bleiben Sie, wenn Sie während eines vertraulichen Gesprächs den Assistenten ausschalten.

7. Schützen Sie Informationen, die einer besonderen Verschwiegenheitspflicht unterliegen (z.B., berufsrechtlichen Verschwiegenheit, Bankgeheimnis, Gesundheitsdaten oder weiteren Daten besonderer Kategorien des Art. 9 Abs. 1 DS-GVO) besonders.

8. Bewahren Sie nach Arbeitsende alle vertraulichen Unterlagen und mobilen Datenträger verschlossen auf.

9. Entsorgen Sie vertrauliche Unterlagen nicht im Papierkorb, sondern verwahren Sie sie verschlossen, bis Sie diese im Entsorgungscontainer oder Shredder Ihres Unternehmens/Ihrer Behörde sicher vernichten können.

10. Bei Fragen können Sie sich an folgende Personen wenden: NAME Ansprechpartner (z.B. aus der Informationssicherheit oder des/ der Datenschutzbeauftragten).

[1] Ein spezieller USB-Stick baut in der privaten Hardware ein zweites, virtuelles System auf. Die private Software des Endgeräts wird somit nicht genutzt.

[2] Eine Zwei-Faktor-Authentifizierung schützt Zugänge mit Hilfe von „Besitz und Wissen", z.B. eines Benutzernamens und eines Passworts sowie einer zusätzlichen weiteren Sicherheitsabfrage. Diese zusätzliche Sicherheitsabfrage kann z. B. durch einen Security-Token erfolgen oder eine Information, die über ein weiteres Gerät zugestellt wird, z.B. über eine App oder eine sms auf das Smartphone.