ARBEITS- UND DATENSCHUTZRECHT

JANUAR 2022

Hinweise zum Homeoffice

Mit dem „Gesetz zur Änderung des Infektionsschutzgesetz und weiterer Gesetze anlässlich der Aufhebung der Feststellung der epidemischen Lage von nationaler Tragweite“ kam es erneut zu Neuregelungen gerade auch hinsichtlich der Arbeitstätigkeit im Homeoffice. Ab dem 22.11.2021 und befristet bis zum 19.03.2022 wird die generelle Homeoffice-Pflicht für Büromitarbeiter wieder eingeführt, sofern keine zwingenden betrieblichen Gründe oder Gründe auf Arbeitnehmerseite entgegenstehen. Beschäftigte haben dieses Angebot anzunehmen, soweit ihrerseits keine Gründe entgegenstehen. Dabei handelt es sich um dieselbe Regelung, die bereits vom 23.04.2021 bis zum 30.06.2021 schon einmal galt.

Die Wiedereinführung der Homeoffice-Pflicht stellt Betriebe aber weiterhin vor erhebliche Herausforderungen, da eine Vielzahl damit verbundener Fragen ungeklärt ist. Die Parteien eines Arbeitsverhältnisses müssen aber wissen, was datenschutzrechtlich im Homeoffice erlaubt ist und was nicht. In einem Infopaket „Homeoffice“ des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (LfD Sachsen-Anhalt) finden sich nunmehr u. a. Hinweise und eine Checkliste zur Umsetzung der datenschutzrechtlichen Anforderungen für das Arbeiten im Homeoffice:

- https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Hinweise_Homeoffice.pdf

- https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Checkliste_Homeoffice.pdf

Ergänzt werden diese Hinweise durch Informationen des Bundeskriminalsamts (BKA) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur technischen Sicherheit, insbesondere zum Thema Cyberkriminalität, also Angriffe auf Unternehmen und Behörden aus dem Internet.

Auf einige dieser Fragen soll– ohne Anspruch auf Vollständigkeit – nachstehend eingegangen werden.

a)

Ist vor der Einrichtung von Telearbeit für eine konkrete Aufgabe jeweils geprüft worden, ob die Verarbeitung von personenbezogenen Daten im häuslichen Bereich erforderlich ist bzw. ob Alternativen gegeben sind?

Im Hinblick auf das Schutzgebot aus Art. 1 Abs. 1 DSGVO und das Gebot der Datenminimierung ist vor der Einrichtung von Homeoffice und Telearbeit zu prüfen, ob die Arbeitsabläufe organisatorisch so geregelt werden können, dass sich für die auszulagernde Arbeit die Möglichkeit ergibt, auf personenbezogene Daten zu verzichten bzw. möglichst wenig Daten mit Personenbezug zu verarbeiten.
Weiter ist zu prüfen, ob es möglich ist, den zu verarbeitenden Datenbestand zu anonymisieren oder zumindest zu pseudonymisieren.

b)

Sind für die jeweilige Aufgabe und die Art bzw. Kategorie der anfallenden Daten gesondert die Sensibilität der Daten, das Risiko durch die Art der vorgesehenen Verarbeitung und die gebotenen Schutzmaßnahmen geprüft worden? Ist diese Prüfung für die jeweilige Aufgabe dokumentiert worden?

Es ist stets vor der Auslagerung eine sorgfältige Prüfung der vorgesehenen Datenverarbeitungen durchzuführen, insbesondere in Bezug auf mögliche Auswirkungen im Fall eines Missbrauchs bzw. einer Verletzung der Sicherheit der Datenverarbeitung. Nach Art. 24 Abs. 1 DSGVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Jeweils im Einzelfall sind für die zu verarbeitenden Daten der Schutzbedarf und das Risiko zu prüfen, um die erforderlichen Maßnahmen festzulegen, die das Risiko auf ein angemessenes Maß reduzieren. Weiter ist zu berücksichtigen, dass der Verantwortliche die grundverordnungskonforme Verarbeitung auch nachzuweisen hat, sodass eine Dokumentation der Prüfung sinnvoll ist.

c)

Welche Arten von personenbezogenen Daten werden in Telearbeit verarbeitet?

Es sollte vorab festgelegt sein, was für Daten (Gesundheitsdaten, Einkommensdaten, Kontaktdaten, Verhaltensweisen, Steuerdaten etc.) auf welchen Datenträgern in welcher Weise verarbeitet werden dürfen.

Ein besonderer Schutzbedarf kann sich ergeben, wenn besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO, u. a. Gesundheitsdaten, rassische und ethnische Herkunft, biometrische Daten) verarbeitet werden. Ein erhöhter Schutzbedarf kann sich auch aus einer gesetzlich bzw. berufsständisch gebotenen Verschwiegenheits- bzw. Schutzpflicht ergeben, wie beispielsweise in Bezug auf Personalaktendaten (Personalaktengeheimnis) oder Sozialdaten (Sozialdatengeheimnis).

d)

Sind Beschäftigte, die Telearbeit verrichten, zuvor bezüglich der erhöhten Risiken und gebotenen Schutzmaßnahmen sensibilisiert worden? Gibt es allgemeine Vorgaben zur Einrichtung des häuslichen Arbeitsplatzes? Ist eine Regelung zur Versendung dienstlicher E-Mails an private E-Mail-Postfächer erfolgt?

Über die regelmäßige Schulung bzw. Fortbildung zu datenschutzrechtlichen Aspekten hinaus ist es notwendig, für die hinreichende Sensibilität der in Homeoffice/Telearbeit Tätigen Sorge zu tragen. Dafür bleibt der Verantwortliche auch bei Verarbeitung außer Haus in der Verantwortung.

Auch der häusliche Arbeitsplatz muss angemessene Sicherheiten bieten. Dazu kann beispielsweise vorgegeben werden, unbefugte Einsichtnahmen, z. B. durch Mitbewohner oder Besucher, zu vermeiden, Unterlagen nach Arbeitsende vom Schreibtisch zu entfernen und sicher zu verschließen, das Mithören unbefugter Personen zu vermeiden oder dienstliche/betriebliche Datenbestände von privaten Daten zu trennen.

Besonderer Aufmerksamkeit bedarf das Öffnen von Links und Dokumenten, die ungewohnt erscheinen, da die Telearbeit u. U. nicht von den Schutzmaßnahmen zentraler Systeme profitiert.

Die Beschäftigten sollten spezifische Gefahren kennen, wie z. B. bezüglich unsicherer Transporte oder unzureichender Vernichtung. Sie sollten hinsichtlich der Vorgaben und der einzuhaltenden Verfahren instruiert werden. Einzuhaltende Sicherheitsmaßnahmen sollten genau beschrieben werden. Dies sollte im Rahmen einer schriftlichen Anweisung erfolgen. Durch entsprechende Vorgaben wird die weisungsgemäße Verarbeitung personenbezogener Daten umgesetzt und gleichzeitig dem Schutz von Geschäftsgeheimnissen Rechnung getragen. Ergänzend dient dies dem gebotenen Nachweis organisatorischer Maßgaben (Art. 5 Abs. 2 DSGVO).

Eine Weiterleitung von dienstlichen E-Mails an private Postfächer erscheint problematisch und sollte entfallen. Die für ggf. sehr sensible Daten gebotene umfassende Sicherung des digitalen Transports, die Sicherung der Verfügbarkeit und des Schutzes vor Zugriffen Fremder auf das private Postfach, wie z. B. sichere Verschlüsselungen, sind nur bedingt und durch den Arbeitgeber direkt gar nicht zu gewährleisten.

e)

Ist für die Telearbeit auch die Nutzung privater (End-) Geräte vorgesehen bzw. gestattet?

Professionell administrierte Technik gewährleistet in hohem Maße Datensicherheit (z. B. in Bezug auf Firewall, Virenschutz, Malwareschutz, sichere Verbindungen, Verschlüsselungen). Für private Geräte dürfte wohl nur in Ausnahmefällen gewährleistet sein, dass die Konfiguration den dienstlichen Sicherheitsanforderungen hinreichend Rechnung trägt. Dem Verantwortlichen ist in der Regel nicht die Möglichkeit gegeben, die Installation und Konfiguration der genutzten privaten Geräte sowie notwendige Aktualisierungen von (Sicherheits-)Software zu steuern und zu prüfen. Private Geräte sind oft mit Anwendungen versehen, die sich bei der Installation umfassende Zugriffsrechte haben gewähren lassen. Mit der Nutzung von privaten Geräten im privaten Umfeld erhöht sich auch die Gefahr, dass diese mit Schadsoftware infiziert werden.

Auf die Nutzung privater Endgeräte sollte daher, auch im Interesse der Vermeidung von Haftungsproblemen, verzichtet werden.

f)

Wie, wie oft, in welchem Umfang und durch wen erfolgen Kontrollen hinsichtlich der Einhaltung der technischen und organisatorischen Vorgaben?

In Bezug auf technische und organisatorische Maßnahmen ist zu berücksichtigen, dass sich die Anforderungen im Laufe der Zeit beispielsweise infolge von technischen Entwicklungen ändern. Die Sicherung der Einhaltung organisatorischer Vorgaben kann ggf. die Überprüfung erfordern. Gemäß Art. 24 Abs. 1 Satz 2 DSGVO sind getroffene Maßnahmen daher erforderlichenfalls zu überprüfen und zu aktualisieren.

Der Datenschutzbeauftragte muss Kontrollmöglichkeiten haben (Art. 39 Abs. 1 lit. b) DSGVO). Ihm muss daher notfalls auch ein Zugang zum häuslichen Bereich möglich sein. Ein Zutritt zu Privatwohnungen ist jedoch grundsätzlich ausgeschlossen. Eine Verlagerung in den privaten Bereich darf die Verarbeitung aber nicht der Kontrolle entziehen. Um die von der DSGVO geforderten Kontrollen zu ermöglichen, bedarf es daher der Zustimmung der zu Hause Beschäftigten. Dazu ist vorab die Zustimmung des Beschäftigten einzuholen. Weiter ist im Hinblick auf die Auswirkung des Schutzes des Wohnungsgrundrechts (Art. 13 Abs. 1 GG) zu beachten, dass auch eventuelle Mitbewohner einverstanden sein müssen. Bei Widerruf der Zustimmung bzw. einer Zutrittsverweigerung ist die Telearbeit daher einzustellen.

Praxishinweis

In den Hinweisen zum Homeoffice werden diese und weitere Empfehlungen und Notwendigkeiten zur Verarbeitung personenbezogener Daten dargestellt, die bei der Einrichtung von Homeoffice-Arbeitsplätzen unbedingt bedacht werden sollten.

Darüber hinaus sollte zwingend eine schriftliche Vereinbarung zwischen den Parteien des Arbeitsvertrages über die (vorübergehende) Tätigkeit im Homeoffice geschlossen werden. Insbesondere derartige Befristungen bedürfen zu ihrer Wirksamkeit der Schriftform.