Nutzung von Homeoffice oder Telearbeit

Das Datenschutzrecht gilt grundsätzlich auch für das Arbeiten im Homeoffice. Jeder Einzelfall ist zu prüfen und unter Beachtung des Schutzbedarfs der zu verarbeitenden Daten zu beurteilen, ob die Bearbeitung im Homeoffice datenschutzrechtlich vertretbar ist. Zu entscheiden hat das die datenschutzrechtlich verantwortliche Stelle.

Risiken lassen sich weder bei der Arbeit im Büro, noch im Homeoffice gänzlich vermeiden. Mit der Verlagerung der Arbeitsstätte in den häuslichen oder gar in den öffentlichen Bereich steigen jedoch die Risiken, da die Kontroll- und Einflussmöglichkeiten der verantwortlichen Stelle eingeschränkt sind. Vertretbar ist die Verarbeitung personenbezogener Daten, wenn deren Schutz durch angemessene technische und organisatorische Maßnahmen gewährleistet ist. Kann aber z.B. der erhöhte Schutzbedarf für Sozialdaten oder Beschäftigtendaten nicht gewährleistet werden, dürfen derartige Daten auch nicht im Homeoffice verarbeitet werden.

Bei der Beurteilung, ob personenbezogene Daten außerhalb der Diensträume verarbeitet werden dürfen, sind auch Arbeitsabläufe und Kommunikationswege zu berücksichtigen. Kann die Aufgaben– und Ergebnisübermittlung durchgängig automatisiert auf elektronischem Weg erfolgen oder muss ein physischer Transport von Unterlagen durchgeführt werden? Bei Letzterem kann das Risiko eines Verlustes steigen und unbefugte Dritte können auf personenbezogene Daten zugreifen. Gleiches gilt bei Verlust eines Notebooks oder Smartphones, wenn die Geräte nicht verschlüsselt und gesperrt sind.

Allgemeingültige Regelungen für eine rechtssichere Gestaltung von Homeoffice lassen sich nur begrenzt treffen. Die folgende Checkliste führt mögliche Regelungsbereiche und Einzelhinweise auf, die bei einer individuellen Gestaltung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu bedenken sind. Weitere Informationen zu technischen Fragen rund um das Home Office finden Sie unter: https://it.landeskirche-hannovers.de/homeoffice .

1. Organisatorische Regelungen

- Datenschutzgrundsätze sind in einer Dienstvereinbarung zu regeln und mit den Mitarbeitenden bzw. Mitarbeitervertretung vertraglich zu vereinbaren.
- Die zu verarbeitenden Daten sind zu klassifizieren und die einzuhaltenden Sicherheitsmaßnahmen zu beschreiben.
- Allgemeine Sicherheitsanforderungen für z.B. Datensicherung, Virenschutz, Firewall, Verschlüsselung von Datenträgern, Komplexität von Passworten, abschließbare Schränke sind festzulegen.
- Eine private Nutzung dienstlicher Geräte oder dienstliche Nutzung privater Geräte ist zu regeln oder auszuschließen.
- Regelungen zur Datenübermittlung oder Fernzugriffe über Virtual Private Network (VPN), sowie Umgang mit mobilen Datenträgern (z.B. USB) oder Ausdrucken sind zu regeln.
- Die Vorgehensweise bei evtl. Datenpannen im Homeoffice ist zu bestimmen.
- Zu nutzende Kommunikationsarten und -wege (E-Mail, Internet, Mobiltelefon) sind vorzugeben.
- Regelungen zur Datenträgervernichtung (Papier und elektronische) sind abzustimmen.
- Ausgabe und Rücknahme dienstlicher Geräte (z. B. Notebook, Smartphone) und Akten sind zu dokumentieren.

- Ein Zutrittsrecht der verantwortlichen Stelle zum Heimarbeitsplatz oder der dazu beauftragten Personen zwecks Kontrolle und Zugriff auf dienstliche Dokumente, ist zu vereinbaren. Dazu gehört auch die Zustimmung der in der häuslichen Gemeinschaft lebenden Personen.
- Durchführung regelmäßiger Schulungen zum sicheren und datenschutzgerechten Umgang mit PCs und mobilen Geräten.
- Örtliche Datenschutzbeauftragte sollten in die Erstellung der Regelungen zum Homeoffice/Telearbeit einbezogen werden.
- Alle Regelungen zum Homeoffice/Telearbeit sind den betroffenen Mitarbeitenden bekanntzugeben.

2. Arbeitsabläufe

- Transport mobiler Geräte erfolgt ausschließlich im gesperrten Zustand.
- Papierunterlagen und dienstlich genutzte Geräte dürfen nicht unbeaufsichtigt gelassen werden, so dass Dritte keine Möglichkeit der Einsichtnahme bekommen. Dies gilt auch für den Transport.
- Drucker nur anbinden, wenn Dritte keine Kenntnis von den Ausdrucken erlangen können.
- Dienstliche Telefonate sollen nur geführt werden, wenn keine unbefugten Dritten mithören können.
- Bei Nutzung privater Telefone müssen automatisch gespeicherte Anrufkontakte regelmäßig gelöscht werden. Die eigene private Rufnummer sollte unterdrückt sein.
- Bei Nutzung von Smartphones dürfen Dritte (z.B. über installierte Apps) nicht auf berufliche Kontakte des Telefonbuchspeichers zugreifen können.
- Dienstliche E-Mails dürfen nicht auf private Postfächer umgeleitet werden.

3. Zugriffskontrolle

- Für eine sichere Authentisierung sind Passwort (ausreichend komplex) oder PIN zu verwenden.
- Authentisierung, Zugriffe, Änderungen und Administratortätigkeiten werden protokolliert.
- Benutzerrechte für Mitarbeitende einschränken (keine Administratorenrechte).
- Verbindung zur Dienststelle nur über dienstlich bereitgestelltes Virtual Private Network (VPN).
- Der Umgang mit USB-Anschlüssen muss geregelt werden, z.B. Verbot des Anschlusses von USB-Sticks.

4. Datensicherheit (Verschlüsselung)

- Daten auf mobilen Geräten (Notebook, Smartphone, USB-Stick) sind stets zu verschlüsseln.
- Mail-Anhänge mit personenbezogenen Daten sind zu verschlüsseln.
- Die Verbindung zum häuslichen W-LAN muss verschlüsselt sein oder kabelgebunden erfolgen.

5. Umgebungssicherheit

- Geeignete häusliche Räumlichkeiten und Arbeitsmittel für die sichere Aufbewahrung von Unterlagen, Geräten und Datenträgern müssen vorhanden sein.
- Die in der häuslichen Gemeinschaft lebenden Personen haben keinen Zugriff auf dienstliche Geräte und Unterlagen.

- Clean-Desk-Methode wird eingehalten (Dokumente vor Einsicht Dritter schützen).
- Bei Nichtnutzung des Computers von 15 Minuten soll sich der Bildschirm automatisch sperren.
- Anm. Collande: Bitte den Satz ändern in: Eine automatische Bildschirmsperre beim Verlassen des Computers ist einzurichten.
- Blickschutzfolie für den Bildschirm schützt vor Blicken Unbefugter (z.B. Besucher, Familienangehörige).

6. Betriebssicherheit

- Mitarbeitende im Homeoffice sollten sicher mit mobilen Geräten umgehen können.
- Updates werden zeitnah installiert und sind stets aktuell.
- Eine Firewall ist aktiviert.
- Ein Virenschutz ist installiert und immer aktuell.
- Die Aktivierung eines zusätzlichen Bot-Schutzes ist wünschenswert.
- Dienstliche Daten sollten auf zentralen Systemen der Dienststelle gespeichert werden (Netzlaufwerke, DMS usw.). Bei lokaler Speicherung ist eine regelmäßig eine verschlüsselte Datensicherung durchzuführen, inkl. einer Kontrolle der Wiederherstellung.

7. Kommunikationssicherheit

- Sicherstellung des Zugriffs auf dienstliche E-Mail-Postfächer. Dienstliche E-Mails dürfen nicht auf private Postfächer umgeleitet werden.
- Vertrauliche Dokumente dürfen nicht unverschlüsselt einer E-Mail angehängt werden.
- Bei Videokonferenzen ist die Nutzung eines Headsets empfehlenswert.
- Die Nutzung öffentlicher Netzzugänge ist nur unter Verwendung von VPN gestattet.
- Ein Mobile Device Management zur zentralen Administration der Endgeräte ist anzustreben (ermöglicht nachträgliches Löschen der Daten eines verlorenen oder gestohlenen Gerätes).