Die Landesbeauftragte für den Datenschutz Niedersachsen

Hilfestellung zum Datenschutz im Homeoffice – Stand: Juli 2020

Viele Unternehmen, freiberuflich Tätige, Selbstständige, Behörden und sonstige öffentliche Stellen fragen sich nicht erst seit der Corona-Pandemie, wie sie die Arbeit von zu Hause datenschutzkonform gestalten können. Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen gibt Hinweise zum Umgang mit personenbezogenen Daten bei der Arbeit im sog. Homeoffice.

Analyse vor Einführung des Homeoffice[1]

Bei der Festlegung, was im Homeoffice bearbeitet werden darf und was nicht, obliegt es dem/der Verantwortlichen (i. d. R. das Unternehmen, die Organisation die Behörde), **Art, Umfang, Umstände und Zwecke** der jeweiligen Verarbeitung festzulegen. Unter Berücksichtigung dieser Voraussetzungen müssen in einer **Risikoanalyse** die Gefährdungen für die Rechte der Betroffenen, die jeweilige Schadenshöhe und die Eintrittswahrscheinlichkeit untersucht werden.[2] Auf Grundlage des ermittelten Risikowertes, in Abwägung mit den Implementierungskosten und unter Berücksichtigung des Standes der Technik, muss der/die Verantwortliche schließlich **wirksame und angemessene technische und organisatorische Maßnahmen (TOM)** festlegen und implementieren. Diese müssen den Schutz der Verarbeitung gewährleisten, indem sie die Risiken auf ein vertretbares Maß reduzieren. Es müssen also in jedem Fall **vor dem Beginn der Tätigkeit im Homeoffice** die dem Risiko, der Arbeitssituation und dem Verarbeitungskontext entsprechenden Prüfschritte absolviert und Vorarbeiten geleistet werden (Art. 5, 24, 25, 32 Datenschutz-Grundverordnung - DS-GVO).

Wurde die Telearbeit bzw. das mobile Arbeiten z. B. im Zuge von Corona neu eingeführt, sollten **Regelungen zu Datenschutz und -sicherheit** im Homeoffice getroffen und diese den Beschäftigten verständlich und nachvollziehbar erläutert werden.

Bei Telearbeit i.S.v. § 2 Abs. 7 Arbeitsstättenverordnung bedarf es einer **individualvertraglichen Vereinbarung** zwischen dem Arbeitgeber/der Arbeitgeberin und dem/der Beschäftigten, in der mindestens die wöchentliche Telearbeitszeit sowie die Geltungsdauer der Vereinbarung zu regeln sind. Im Bereich der niedersächsischen Landesverwaltung sind zudem die Vereinbarung gemäß § 81 Niedersächsisches Personalvertretungsgesetz (NPersVG) über Telearbeit in der Landesverwaltung[3] sowie eventuell bestehende Dienstvereinbarungen nach § 78 NPersVG, die Regelungen zum Homeoffice beinhalten, zu beachten. Auch für alle übrigen Formen der Nutzung des Homeoffice wird der Abschluss einer Vereinbarung empfohlen.

---

[1] Der Begriff „Homeoffice“ ist nicht definiert und wird als Oberbegriff für Telearbeit sowie sonstige Formen des mobilen Arbeitens verwendet;
[2] Vgl. Handlungsempfehlung für Praktiker zum technisch-organisatorischen Datenschutz, https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html
[3] Beschluss der Landesregierung vom 14.12.2004, Nds. MBl. 2005 S. 160;

Wegen der nach Art. 13 Grundgesetz garantierten Unverletzlichkeit der Wohnung hat der Arbeitgeber/die Arbeitgeberin **kein generelles Zugangsrecht zu Wohnungen von Beschäftigten**. Deshalb bedarf es für den Zugang zur Wohnung einer wirksamen Einwilligung des/der Beschäftigten.

Datenschutz zu Hause – so geht es

- Vor Ort muss ein **geeigneter Arbeitsplatz** gefunden werden, an dem Dokumente mit personenbezogenen Daten sicher aufbewahrt werden können. Empfehlenswert ist ein **eigener abschließbarer Raum**, der nach Feierabend oder in Pausen für Dritte nicht zugänglich ist. Ist das räumlich nicht möglich, sollten sämtliche Unterlagen zumindest in einem **abschließbaren Schrank oder Rollcontainer** aufbewahrt werden.
- In jedem Fall ist bei der Heimarbeit darauf zu achten, dass sich **berufliche und private Daten nicht mischen** und keine unberechtigte Person Zugriff auf die dienstlichen Daten hat. Sämtliche genutzten Geräte müssen daher über einen **geeigneten sicheren Passwortschutz** (z. B. starkes Passwort) oder ein anderes geeignetes **Authentifizierungsverfahren** (z.B. Token, Chipkarte)[4] sowie **verschlüsselte Speicher** verfügen.
- **Bildschirme** müssen so stehen, dass Unbefugte keinen Einblick nehmen können, ggf. kann ein sog. Blickschutzfilter nützlich sein.
- Beim (auch kurzfristigen) **Verlassen des Arbeitsplatzes** müssen eine **Bildschirmsperre** (z. B. mittels Bildschirmschoner) und ein Passwort-/Authentifikationsschutz aktiviert werden.
- An einem dienstlichen Gerät sollten überdies **keine private Hardware angeschlossen** werden (z. B. Tastaturen, USB-Sticks oder Festplatten), um das Infektionsrisiko mit Schadsoftware zu verringern.
- Wie im geschäftlichen Umfeld üblich, sind auch im Homeoffice die Daten **regelmäßig zu sichern**. Dazu sollte ein einheitliches Datensicherungskonzept (Backup- und Recovery-Verfahren) eingesetzt werden.
- Dienstliche **Papierdokumente** sollten zwischen Arbeitsstätte und Homeoffice **in verschlossenen Behältern** transportiert werden. Zudem dürfen sie nicht im privaten Papiermüll entsorgt, sondern nach den jeweiligen Bestimmungen des Unternehmens **vernichtet** werden. Steht am heimischen Arbeitsplatz etwa kein Schredder zur Verfügung, sind die Dokumente mit ins Büro zu nehmen und dort zu vernichten.
- **Telefonate und Videokonferenzen** mit vertraulichem Inhalt sind so zu führen, dass andere Haushaltsmitglieder, Besucher, Nachbarn oder andere unbefugte Personen den Inhalt des Gesprächs nicht wahrnehmen können. Hierbei sind auch geöffnete Fenster zu berücksichtigen. Balkon, Terrasse oder Garten eignen sich grundsätzlich nicht für solche Gespräche.
- Auch evtl. vorhandene **digitale Assistenten**, welche über Sprache reagieren, sollten ausgeschaltet bzw. entfernt werden.

[4] Weitere Informationen in der Handlungsempfehlung sichere Authentifizierung;

Technische und organisatorische Maßnahmen (TOM)

Verantwortliche müssen der im Vergleich zum betrieblichen Arbeitsplatz veränderten Gefährdungslage im Homeoffice Rechnung tragen und sicherstellen, dass das Schutzniveau angemessen ist. Abhängig von den jeweils identifizierten Gefährdungen und Risiken kommen insbesondere folgende Maßnahmen in Betracht (nicht abschließend):

- Vom Arbeitgeber bereitgestellte **Endgeräte** sollten ebenso **zentral administriert** und einer einheitlichen Policy unterworfen werden wie Endgeräte in der Betriebsstätte. Damit muss ein regelmäßiges **Update- und Patchmanagement** sichergestellt werden sowie regelmäßige **Updates von Signaturen** für die Endgeräte.
- **Zugang** der Berechtigten zu den sensiblen personenbezogenen Daten **nur mit PIN und hardwarebasiertem Vertrauensanker** (Zwei-Faktor-Authentifizierung).
- Verbindung ausschließlich über eine **angemessen abgesicherte Verbindung**, z. B. sogenanntes Virtual Private Network (VPN) über alle Kommunikationswege einschließlich des genutzten heimischen WLAN/WiFi-Netzes sowie der Internetanbindung über Festnetz. **WiFi-Zugänge** müssen **mit einem sicheren Passwort abgesichert** sein.
- Als eine der präsentesten Gefährdungen gilt im heimischen Umfeld die Verletzung der Vertraulichkeit und der Integrität personenbezogener Daten in Arbeitsunterlagen, Datenspeichern und Kommunikationsprozessen (insb. bei Telefonaten, Videokonferenzen, E-Mails, Messenger-Nachrichten, Chat-Kommunikation, gemeinsam bearbeiteten und zwischengespeicherten Dokumenten sowie Metadaten). Diese Daten dürfen unbefugten Dritten nicht zugänglich sein. Für die externe Kommunikation müssen die Absicherungsmaßnahmen dem festgestellten Risikowert entsprechend implementiert werden. Als häufig geeignete Gegenmaßnahme gilt regelmäßig die **Transportverschlüsselung für Datenübertragungen**. Als wirksamste Maßnahme für höheren Schutzbedarf gilt die **Ende-zu-Ende-Verschlüsselung**, bei der die Kontrolle über die Daten und das Schlüsselmanagement nur an den Endstellen liegt, also beim Heimarbeitenden und dem Kommunikationspartner, nicht aber bei Dritten.
- Auf allen **lokalen Datenträgern** (Desktop-PC, Tablet, Laptop, Notebook, USB-Sticks) sollten die Daten **verschlüsselt gespeichert** werden.
- Bei **dienstlichen Smartphones** sollte eine **PIN-Sperre erzwungen** werden.
- Gehen mobile Endgeräte verloren, müssen Sofortmaßnahmen ergriffen werden: z. B. Remote Wipe (Löschung) bei Smartphones, Sperrung von Hardware-Token.
- **Sperrung von USB-Zugängen** und anderen Anschlüssen.
- Keine Anbindung von privaten Druckern.
- Keine private Nutzung der beruflich zur Verfügung gestellten IT-Ausstattung.
- Grundsätzlich **keine berufliche Nutzung privater Endgeräte** (mehr dazu siehe unten).
- Regelmäßige **Schulung / Fortbildung der Beschäftigten** zum datensicheren und datenschutzgerechten Umgang mit mobilen Geräten.

Grundsatz: Keine Nutzung privater Endgeräte

Arbeitgeber/-in oder Dienststelle können nicht die Nutzung privater Endgeräte für die Erbringung der Arbeitsleistung verlangen. Jedoch ist diese **mit Einwilligung der Beschäftigten möglich**. Allerdings muss der Arbeitgeber/die Arbeitgeberin/die Dienststelle (i. d. R. die IT-Abteilung des Unternehmens oder der Behörde) **vor einer Nutzung von Privatgeräten prüfen**, ob das Schutzniveau bei dieser Verarbeitung angemessen ist (siehe Absatz oben „Prüfungen vor Einführung des Homeoffice“). **In der Regel sollte auf die Nutzung privater Endgeräte verzichtet werden**, besonders aufgrund der erhöhten Gefahr der Vermischung privater und beruflicher Daten.

Falls es die in einer Risikoanalyse ermittelten Restrisiken tragbar erscheinen lassen, ausnahmsweise Daten an einem privaten Computer zu verarbeiten, sollte hierfür zumindest ein **extra Konto** eingerichtet und die Daten in einem **verschlüsselten Bereich** gesondert gespeichert werden. Sobald die Daten auf dem dienstlichen Server abgelegt worden sind, sind sie auf dem Privat-PC unwiederbringlich zu löschen. Hierfür reicht es nicht aus, wenn sie lediglich in den Papierkorb verschoben werden. Vgl. hierzu die Anforderungen in Baustein 60 „Löschen und Vernichten“ des Standard-Datenschutzmodells.

Besonders **sensible Daten Dritter** (z. B. Gesundheitsdaten, Daten zu politischen oder weltanschaulichen Ansichten, vgl. Art. 9 DS-GVO) dürfen **nicht auf privaten Geräten** verarbeitet werden.

Quellen und weiterführende Informationen:

https://www.lda.bayern.de/media/best_practise_homeoffice_baylda.pdf

https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Der Landesbeauftragte für den Datenschutz
Niedersachsen Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E.Mail poststelle@lfd.niedersachsen.de