Bayerisches Landesamt für
Datenschutzaufsicht

Datenschutzrechtliche Regelungen bei Homeoffice

Best-Practice-Prüfkriterien

Stand: 18. Mai 2020

Ziel und Inhalt dieses Papiers

Die Corona-Pandemie hat auch viele Unternehmen, Selbstständige und Freiberufler mit der Frage konfrontiert, wie denn die Arbeitsfähigkeit weiterhin sichergestellt und zeitgleich Maßnahmen zur Eindämmung des Infektionsgeschehens getroffen werden können. Bei bestimmten Tätigkeiten führte dies dazu, dass sehr schnell die Arbeit von zu Hause aus erweitert oder erst eingeführt wurde. Nachdem nun einige Wochen im Homeoffice vergangen sind, soll diese Handreichung einen Überblick über die wichtigsten Praxismaßnahmen im Homeoffice entsprechend den geltenden gesetzlichen Datenschutzvorgaben geben. Im Sinne einer gezielten Prävention von Datenschutzverstößen soll damit im momentanen „neuen Alltag" eine gesteigerte Sensibilisierung für dieses Thema erreicht und mit konkreten Prüffragen der eigene Stand der Umsetzung unterstützt werden. Die aufgeführten **Prüfpunkte sind nicht als abschließend zu betrachten**, sondern stellen einen **Best-Practice-Ansatz** dar, der bspw. von Seiten der Geschäftsführung oder des Datenschutzbeauftragten im Sinne einer Soll-Ist-Überprüfung verwendet werden kann. Dabei ist es nicht bei allen Punkten immer der Fall, dass diese umgesetzt werden müssen – dann ist jedoch eine kurze kritische Hinterfragung des Grundes samt kurzer Dokumentation angeraten.

Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice

1 Arbeitsumgebung

Bei der Arbeit zu Hause soll die Umgebung so ausgestaltet sein, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist

- ☐ Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook oder in die Papierunterlagen werfen können
- ☐ Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages
- ☐ Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist (bspw. Schreibtisch am Fenster in Parterrewohnung)
- ☐ Papierunterlagen können in Dokumentenmappen oder Schränken verschlossen werden
- ☐ Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
- ☐ Sperrung des Notebooks bei Verlassen des Arbeitsplatzes falls ein anderer Zugriff (z. B. Kinder, Katze) nicht ausgeschlossen ist
- ☐ Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz, ...)

2 Genutzte Hardware

Es wird die Bereitstellung von dienstlichen Geräten empfohlen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.

- ☐ Dienstliche Notebooks werden gestellt
- ☐ Dienstliche Smartphones oder Softphones werden gestellt
- ☐ Bei Verwendung von Privatgeräten werden Remoteverbindungen auf Terminalserver verwendet
- ☐ Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt

3 Umgang mit Papierdokumenten

Noch nicht alle Arbeitsabläufe sind komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen Risiken, die in den Räumlichkeiten des Büros so nicht auftreten.

- ☐ Papierunterlagen werden in geeigneten Mappen (mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen
- ☐ Regelungen, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant, ...) ausgesetzt werden sollen
- ☐ Entsorgung von Papierunterlagen erfolgt nicht über den Hausmüll, sondern entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 (nach DIN 66399)
- ☐ Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert und es wird bei solchen Dokumenten mit Kopien gearbeitet, sofern möglich

4 Nutzung von Videokonferenzsystemen

Bei der Auswahl von Videokonferenzlösungen, mit denen Präsenzbesprechungen ersetzt werden sollen, müssen bestimmte Anforderungen beachtet werden:

- ☐ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abgeschlossen
- ☐ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden (z. B. unveränderte EU-Standardverträge oder Privacy-Shield-Zertifizierung bei US-Anbietern)
- ☐ Verwendung einer Transportverschlüsselung (z. B. TLS) nach Stand der Technik

- ☐ Verwendung einer Ende-zu-Ende-Verschlüsselung, sofern Daten mit hohem Risiko besprochen bzw. übertragen werden
- ☐ Zugangsschutz zu Konferenzräumen über Passwörter oder individuelle Einladungslinks
- ☐ Keine Aufzeichnung der Inhalte durch den Anbieter zum Zweck der Qualitätsverbesserung oder sonstiger Auswertung
- ☐ Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten durch den Anbieter (Empfehlung: Deaktivierung)
- ☐ Keine Aufzeichnung der Videokonferenz durch das Unternehmen
- ☐ Deaktivierung von biometrischen Features wie Aufmerksamkeitserkennung, sofern eine solche Verarbeitung angeboten wird
- ☐ Regelungen, wann und durch wen Screen Sharing verwendet wird, sind vorhanden
- ☐ Regelungen zum Zweck und der Speicherdauer (z. B. Löschung bei Beendigung der Konferenz) von Chat-Funktionen sind vorhanden
- ☐ Verwendete Apps leiten keine unzulässigen Tracking-Informationen an die App-Anbieter aus
- ☐ Beteiligung des Personal-/Betriebsrats
- ☐ Beteiligung des Datenschutzbeauftragten
- ☐ Hintergrund eines Nutzers kann softwareseitig unscharf gestellt werden („Blurring“)
- ☐ Es gibt die Möglichkeit eines virtuellen Warteraumes, in dem Teilnehmer bis zu Beginn der Konferenz ohne Audio-/Videoübertragung warten können
- ☐ Es existiert eine Moderatorfunktion zur Steuerung (Screen-Sharing-Option, Stummschaltung, Entfernen von Teilnehmern, ...) der Konferenz

5 Sicherheit

Das Homeoffice ist das virtuelle Büro – die Sicherheitsrisiken erhöhen sich durch die Anbindung an das Internet

- ☐ Anbindung an das Firmennetz mit verschlüsselten VPN-Verbindungen nach Stand der Technik
- ☐ Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung nebst PIN/Passwort (z. B. Hardwaretoken oder (Software-)Zertifikate) bei VPN-Verbindungen
- ☐ Nutzung vom heimischen Wi-Fi mit starken Passwörtern
- ☐ Nutzung öffentlicher Wi-Fi-Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindung
- ☐ Zugriff nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung
- ☐ Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen
- ☐ Regelmäßiges Patch Management erfolgt auch auf dem Homeoffice-Notebook durch Konfiguration von automatischen Sicherheitsupdates
- ☐ Täglich Updates der Virensignaturen auf den Homeoffice-Notebooks
- ☐ Regelungen zum Umgang mit USB-Ports (z. B. Deaktivierung oder Verbot des Anschlusses privater Sticks) wurden getroffen
- ☐ Festplattenvollverschlüsselung bei Notebooks
- ☐ Vollverschlüsselung bei dienstlichen Smartphones
- ☐ Pin-Sperre bei dienstlichen Smartphones
- ☐ Regelungen im Verlustfall bei mobilen Endgeräten (z. B. Remote Wipe bei Smartphones, Sperrung von Hardware-Token, ...) sind getroffen
- ☐ IT-Abteilung kann bei Fragen und Problemen auch aus dem Homeoffice erreicht werden

6 Nutzung von Cloud-Diensten

Die Zusammenarbeit im Team über das Homeoffice setzt häufig geeignete Softwarewerkzeuge, sog. Collaboration Tools, voraus.

- ☐ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abgeschlossen
- ☐ Transportverschlüsselung (z. B. HTTPS) nach Stand der Technik
- ☐ Ruheverschlüsselung (auf Festplatten des Cloud-Anbieters) nach Stand der Technik
- ☐ Wirksame Löschung von Daten (z. B. bei Beendigung des Vertrages)
- ☐ Prüffähigkeit der technischen und organisatorischen Maßnahmen durch geeignete Dokumente, Zertifizierungen und zumindest der Möglichkeit, auch ein Vor-Ort-Audit durchzuführen
- ☐ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien ausgewählt worden (z. B. unveränderte EU-Standardverträge oder Privacy-Shield-Zertifizierung bei US-Anbietern)
- ☐ Verwendung starker Passwörter für Nutzer
- ☐ Verwendung von Verfahren zur Zwei-Faktor-Authentifizierung bei administrativen Konten
- ☐ Sensibilisierung der Mitarbeiter für Risiken von Phishing-Attacken auf Cloud Konten

7 Nutzung von Messengern

Neben E-Mails werden zunehmend auch Messenger-Systeme für die Unternehmenskommunikation eingesetzt. Die verwendeten Systeme müssen für einen beanstandungsfreien Einsatz die datenschutzrechtlichen Anforderungen erfüllen.

- ☐ Kommunikation der Inhalte erfolgt Transport- und Ende-zu-Ende verschlüsselt
- ☐ Keine Verwendung oder Weitergabe der Verkehrsdaten („Wer wann mit wem kommuniziert“) an den Anbieter für Zwecke wie Werbung oder Profiling
- ☐ Ende-zu-Ende-Verschlüsselung auch von Anhängen wie Bildern oder Textnachrichten
- ☐ Einsatz einer Mobile-Device-Management Lösung zur Steuerung von Kontakt-Uploads an Messenger-Anbieter

8 Allgemeine organisatorische Regelungen

Verlagern Mitarbeiter die Arbeit ins eigene Zuhause, entstehen völlig neue Sicherheitsprobleme, die als Einfallstor für tiefgreifende Cyberangriffe fungieren können. Die Anbindung von Mitarbeitern im Zu-Hause-Modus muss daher durchdacht und sicher ausgestaltet werden.

- ☐ Überblick über die Mitarbeiter im Homeoffice
- ☐ Überblick über die Geräte der Mitarbeiter im Homeoffice
- ☐ Schulung/Informationen für Mitarbeiter über die Home-office-Regelungen
- ☐ Schriftliche Verpflichtung der Mitarbeiter, dass diese sich an die Regelungen halten – eine Vor-Ort-Kontrolle kann so i. d. R. entfallen
- ☐ Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten
- ☐ Bei sensitiven Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern im Büro die Einsicht durch andere Mitarbeiter

Aktuelle Version zum Download:

www.lda.bayern.de/best_practise_homeoffice

Herausgeber und Kontakt:

Bayerisches Landesamt für Datenschutzaufsicht
(BayLDA) | Promenade 18 | 91522 Ansbach
www.lda.bayern.de | Tel.: 0981 180093-100
poststelle@lda.bayern.de