Bayerisches Landesamt für
Datenschutzaufsicht

Datenschutzrechtliche Regelungen bei Homeoffice

Checkliste mit Prüfkriterien nach DS-GVO

Stand: 22. Juli 2020

Ziel und Inhalt dieses Papiers

Die Corona-Pandemie hat viele Unternehmen, Selbstständige und Freiberufler mit der Frage konfrontiert, wie die Arbeitsfähigkeit weiterhin sichergestellt und zeitgleich Maßnahmen zur Eindämmung des Infektionsgeschehens getroffen werden können. Bei bestimmten Tätigkeiten führte dies dazu, dass das Arbeiten von zu Hause aus sehr schnell erweitert oder neu eingeführt wurde. Diese Handreichung soll hierfür einen Überblick über die wichtigsten Praxismaßnahmen im Homeoffice entsprechend den geltenden gesetzlichen Datenschutzvorgaben geben. Im Sinne einer gezielten Prävention von Datenschutzverstößen soll damit im „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 immer bei allen Punkten der Fall, dass diese umgesetzt zwangsläufig werden müssen – dann ist jedoch eine kritische Hinterfragung des Grundes samt kurzer Dokumentation angeraten.

Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice

1 Arbeitsumgebung

Die Arbeitsplatzumgebung zu Hause soll 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 und 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 – egal ob gewollt oder ungewollt z. B. durch Kinder oder Haustiere – 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

In vielen Betrieben sind noch nicht alle Arbeitsabläufe komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen neue Risiken, die in den Räumlichkeiten des Büros nicht auftraten.

- ☐ Papierunterlagen werden in geeigneten Mappen (u. a. mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen
- ☐ Regelungen bestehen, 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 eigenen Hausmüll, sondern fachgerecht entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 3 (nach DIN 66399)
- ☐ Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert – es wird bei solchen Dokumenten, sofern möglich, mit Kopien gearbeitet

4 Nutzung von Videokonferenzsystemen

Bei der Auswahl von Videokonferenzlösungen, mit denen Präsenzbesprechungen teilweise oder vollständig ersetzt werden, müssen bestimmte Anforderungen beachtet werden.

- ☐ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen
- ☐ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden; es werden hierbei insbesondere die aktuelle Entwicklungen und Veröffentlichungen zur Privacy-Shield-Zertifizierung bei US-Anbietern verfolgt

- ☐ 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 Videokonferenzen 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
- ☐ Bei Bedarf: 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 Moderator-Funktion zur Steuerung der Konferenz (Screen-Sharing-Option, Stummschaltung, Entfernen von Teilnehmern, …)

5 Sicherheit

Das eigene Homeoffice gilt als virtuelles Büro. Durch die Anbindung an das Internet erhöhen sich dabei die Sicherheitsrisiken enorm. Technische Lösungen helfen, diese Risiken zu minimieren.

- ☐ 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 WLAN mit starken Passwörtern
- ☐ Nutzung öffentlicher WLAN-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) wurden getroffen
- ☐ IT-Abteilung kann bei Fragen und Problemen auch aus dem Homeoffice erreicht werden

6 Nutzung von Cloud-Diensten

Im Homeoffice setzt die Zusammenarbeit im Team häufig geeignete Softwarewerkzeuge, sog. Collaboration Tools, voraus. Diese können unter bestimmten Voraussetzungen eingesetzt werden.

- ☐ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen
- ☐ Verwendung einer 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 vorhanden; es werden hierbei insbesondere die aktuelle Entwicklungen und Veröffentlichungen zur Privacy-Shield-Zertifizierung bei US-Anbietern verfolgt
- ☐ 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 Messenger-Diensten

Neben E-Mails werden zunehmend auch Messenger-Systeme für die Unternehmenskommunikation eingesetzt. Die verwendeten Dienste müssen für einen aus Datenschutzsicht beanstandungsfreien Einsatz bestimmte 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

Die Anbindung von Mitarbeitern im Zu-Hause-Modus muss durchdacht und sicher ausgestaltet werden. Neben technischen Lösungen helfen organisatorische Regelungen, um Einfallstore für tiefgreifende Cyberangriffe zu verhindern.

- ☐ 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/checkliste_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