Solidaris
Nutzen stiften – mit Freude für Menschen

Selbst-Check: Datenschutz im Home-Office

Sind Sie vorbereitet auf die Anforderungen?

Sind Sie sowie Ihre Mitarbeiterinnen und Mitarbeiter auf die datenschutzrechtlichen Anforderungen im Home-Office vorbereitet? Machen Sie den Selbst-Check. Erfahren Sie, mit welchen Praxis-Maßnahmen Sie die geltenden gesetzlichen Datenschutzvorgaben umsetzen können. Sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter für das Thema, um so möglichen unbewussten Datenschutz-Verstößen vorzubeugen. Insbesondere der Geschäftsführung und dem/der Datenschutzbeauftragten hilft unsere Checkliste dabei, mögliche Schwachstellen aufzudecken. Sie basiert auf Best-Practice-Ansätzen um einen Soll-Ist-Abgleich durchzuführen. Somit gilt sie sowohl für den weltlichen (DS-GVO) als auch den kirchlichen Bereich (KDG, KDR-OG, DSG-EKD). Nicht alle Punkte sind dabei zwingend umzusetzen. Sollten Abweichungen auftreten, empfehlen wir jedoch die kritische Hinterfragung samt kurzer Dokumentation.

1. Arbeitsumgebung

Stellen Sie die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro her.

- ☐ Familienmitglieder oder Besucher können keinen Blick auf Notebook und Papierunterlagen werfen
- ☐ Clean-Desk-Policy gilt am Ende des Arbeitstages
- ☐ Verwendung von Sichtschutzfolien oder ausreichende Entfernung einhalten, wenn erforderlich (bspw. Schreibtisch am Fenster in Parterrewohnung)
- ☐ Verschließbare Dokumentenmappen oder Schränke stehen für Papierunterlagen zur Verfügung
- ☐ Der Heimarbeitsplatz-Raum wird abgeschlossen, wenn er verlassen wird. Oder betriebliche Unterlagen werden in einem Schrank/einer Aktentasche eingeschlossen
- ☐ Beim Verlassen des Arbeitsplatzes werden Fenster und Türen in Erdgeschosswohnungen immer geschlossen. In höherliegenden Wohnungen gilt dies ebenfalls, wenn diese ohne Weiteres erreicht werden können (z.B. gemeinsamer Balkon o.ä.)
- ☐ Das Notebook wird bei Verlassen des Arbeitsplatzes gesperrt, falls ein fremder Zugriff nicht ausgeschlossen ist
- ☐ Telefongespräche können nicht von unbefugten Personen mitgehört werden (z.B. offenes Fenster, laufende andere Videokonferenz)
- ☐ Dritten werden keine Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z.B. Chipkarten) mitgeteilt oder zugänglich gemacht (z.B. notierte Passwörter oder Lagerung der Chipkarte am Lesegerät)
- ☐ Betriebliche Daten werden auf vom Arbeitgeber zugelassenen Medien gespeichert (z.B. betrieblicher Server)

2. Hardware

Es sollten dienstliche Geräte bereitgestellt werden.
Nutzung von Privatgeräten nur in Ausnahmefällen gestatten.

- ☐ Dienstliche Notebooks sind verfügbar und werden gestellt
- ☐ Dienstliche Smart- oder Softphones sind verfügbar und werden gestellt
- ☐ Bei Verwendung von Privatgeräten: Remoteverbindungen auf Terminalserver wird verwendet und ein Download von dienstlichen Dateien auf dem privaten Rechner technisch ausgeschlossen
- ☐ Keine Nutzung von dienstlich zur Verfügung gestellten Geräten für private Zwecke - auch zu Hause nicht

3. Umgang mit Papierdokumenten

Sollten noch nicht alle Arbeitsabläufe komplett digital nutzbar sein, beachten Sie neue Risiken beim Umgang mit Papierdokumenten, die in Büros nicht auftreten.

- ☐ Es ist mit dem Vorgesetzten abgestimmt, welche Dokumente mit nach Hause genommen werden dürfen
- ☐ Die Mitarbeiterin/der Mitarbeiter transportiert die Dokumente in verschlossenen Behältnissen (z.B. verschlossene Kiste, verschlossener Aktenkoffer)
- ☐ Es werden geeignete Mappen (u.a. mit Unternehmens-Namen im Falle eines Verlustes) bereitgestellt, um Papierunterlagen mit nach Hause zu nehmen
- ☐ Es bestehen Regelungen zur Risiko-Minimierung beim Transport von Papierunterlagen nach/von zu Hause (Vermeidung von Risikosituationen, z.B. Rücksitz beim Einkaufen, Rucksack im Restaurant)
- ☐ Entsorgung von Papierunterlagen nicht über den Hausmüll, sondern fachgerecht entweder im Büro oder zu Hause (Aktenvernichter mind. Sicherheitsstufe 3 nach DIN 66399)
- ☐ Sensibilisierung zu Risiken der Schädigung von wichtigen Papierdokumenten ist erfolgt. Sofern möglich wird mit Kopien gearbeitet.

4. Videokonferenzsysteme

Videokonferenzlösungen müssen gewisse Anforderungen erfüllen, um den Bestimmungen des Datenschutzes gerecht zu werden.

- ☐ Vertrag zur Auftragsverarbeitung mit dem Anbieter ist abgeschlossen
- ☐ Es wurde eine Datenschutz-Information für die Verwendung von Videokonferenz-Systemen zu Verfügung gestellt
- ☐ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden (insbesondere infolge der Unwirksamkeit des EU-US-Privacy-Shields) oder der Anbieter gewährleistet, dass keine Daten in den USA verarbeitet werden
- ☐ Es existiert eine „Hausordnung" zum Umgang mit Videokonferenz-Systemen, in der Verhaltensregeln für die Nutzung festgelegt worden sind
- ☐ Es wird eine Transportverschlüsselung (z.B. TLS bzw. AES 256) nach aktuellem Stand der Technik verwendet
- ☐ Verwendung einer Ende-zu-Ende-Verschlüsselung (insbesondere bei Übertragung/Besprechung von Hoch-Risiko-Daten)
- ☐ Konferenzräume sind Passwort-geschützt oder nur per individuellem Einladungslink erreichbar
- ☐ Es wird keine Aufzeichnung der Inhalte durch den Anbieter zugelassen – zu welchem Zweck auch immer
- ☐ Empfohlen wird eine Deaktivierung von Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten durch den Anbieter
- ☐ Ihr Unternehmen zeichnet keine Videokonferenzen auf
- ☐ Biometrische Features (z.B. Aufmerksamkeitserkennung) sind deaktiviert (falls angeboten)
- ☐ Regelungen, wann und durch wen ScreenSharing 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 weiter
- ☐ Der Personal-/Betriebsrat bzw. die Mitarbeitervertretung ist eingebunden
- ☐ Der Datenschutzbeauftragte ist eingebunden
- ☐ Bei Bedarf: Hintergrund eines Nutzers kann softwareseitig unscharf gestellt werden („Blurring")
- ☐ Ein virtueller Warteraum ist eingerichtet, in dem Teilnehmer bis zum Beginn der Konferenz ohne Audio-/Videoübertragung warten können
- ☐ Es existiert eine Moderator-Funktion zur Steuerung der Konferenz (Screen-Sharing-Option, Stummschaltung, Entfernen von Teilnehmern etc.)

5. Sicherheit

Zur Minimierung der Risiken durch die Internet-Anbindung im Home-Office sollten technische Lösungen eingesetzt werden.

- ☐ Die Anbindung an das Firmennetz ist durch eine VPN-Verbindungen nach Stand der Technik verschlüselt
- ☐ Es wird eine Zwei-Faktor-Authentifizierung nebst PIN/Passwort (z.B. Hardwaretoken oder (Software-)Zertifikate bei VPN-Verbindungen eingesetzt
- ☐ Das heimische WLAN ist mit starken Passwörtern gesichert
- ☐ Öffentliche WLAN-Hotspots werden nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindungen genutzt
- ☐ Zugriff auf für das Home-Office erforderliche Server, Dateiablagen und Anwendungen nur durch die VPN-Verbindung gestatten
- ☐ Speicherung von Daten wird auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen beschränkt
- ☐ Das Patch-Management ist so konfiguriert, dass regelmäßige Sicherheitsupdates automatisch auf den Home-Office-Notebooks installiert werden
- ☐ Die Virensignaturen auf den Home-Office-Notebooks erhalten tägliche Updates
- ☐ Regelungen zum Umgang mit USB-Ports (z.B. Deaktivierung oder Verbot des Anschlusses privater Sticks) wurden getroffen
- ☐ Festplattenvollverschlüsselung bei Notebooks sind eingerichtet
- ☐ Dienstliche Smartphones sind vollverschlüsselt
- ☐ Eine PIN-Sperre ist bei dienstlichen Smartphones eingerichtet
- ☐ Es sind Regelungen bei Verlust von mobilen Endgeräten (z.B. Mobile-Device-Management – Remote Wipe bei Smartphones, Sperrung von Hardware-Token) getroffen
- ☐ IT-Abteilung kann bei Fragen und Problemen auch aus dem Homeoffice erreicht werden

6. Cloud-Dienste

Für den Einsatz von Softwarewerkzeugen für die Team-Zusammenarbeit, sog. Collaboration Tools, sollten die nötigen Voraussetzungen geschaffen werden.

- ☐ Vertrag zur Auftragsverarbeitung mit dem Anbieter ist abgeschlossen
- ☐ Es wurde darauf hingewiesen (z.B. in einer Datenschutz-Richtlinie), welche Unterlagen hochgeladen bzw. nicht hochgeladen werden dürfen
- ☐ Eine Transportverschlüsselung (z.B. HTTPS bzw. SSL) nach aktuellem Stand der Technik wird verwendet
- ☐ Eine Ruheverschlüsselung (auf Festplatten des Cloud-Anbieters) nach Stand der Technik ist verfügbar
- ☐ Die wirksame Löschung von Daten (z.B. bei Beendigung des Vertrages) ist sichergestellt
- ☐ Die technischen und organisatorischen Maßnahmen können durch geeignete Dokumente, Zertifizierungen und zumindest die Möglichkeit von Vor-Ort-Audits geprüft werden
- ☐ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden (insbesondere insbesondere infolge der Unwirksamkeit des EU-US-Privacy-Shields) oder der Anbieter gewährleistet, dass keine Daten in den USA verarbeitet werden
- ☐ Nutzererinnen und Nutzer verwenden starke Passwörter
- ☐ Administrative Konten sind durch Zwei-Faktor-Authentifizierung gesichert
- ☐ Mitarbeiterinnen und Mitarbeiter sind für Risiken von Phishing-Attacken auf Cloud-Konten sensibilisiert

7. Messenger-Dienste

Messenger-Systeme müssen für einen aus Datenschutzsicht beanstandungsfreien Einsatz gewisse Anforderungen erfüllen.

- ☐ Die Kommunikation der Inhalte erfolgt Transport- und Ende-zu-Ende-verschlüsselt
- ☐ Die Verwendung oder Weitergabe der Verkehrsdaten (wer wann mit wem kommuniziert) an den Anbieter für Zwecke wie Werbung oder Profiling ist ausgeschlossen
- ☐ Auch Anhänge wie Bilder oder Textnachrichten sind Ende-zu-Ende-verschlüsselt
- ☐ Bei Verwendung von privaten Geräten: Eine Container-Lösung wird genutzt und neben der Zugriffs-Absicherung des privaten Geräts (PIN, Passwort, Fingerabdruck) wird im Betriebssystem der App-Zugang mittels eigener PIN für die App abgesichert
- ☐ Einer Mobile-Device-Management-Lösung zur Steuerung von Kontakt-Uploads an Messenger-Anbieter wird eingesetzt

8. Allgemeine organisatorische Regelungen

Um Einfallstore für Cyberangriffe zu schließen sollten durchdachte organisatorische Regelungen getroffen werden.

- ☐ Es besteht ein Überblick über die Mitarbeiterinnen und Mitarbeiter im Home-Office
- ☐ Es ist ein Überblick über die Geräte der Mitarbeiterinnen und Mitarbeiter im Home-Office vorhanden
- ☐ Mitarbeiterinnen und Mitarbeiter werden über die Home-Office-Regelungen informiert und geschult
- ☐ Mitarbeiterin/Mitarbeiter unterzeichnet eine schriftliche Verpflichtung, dass sie/er sich an die Regelungen hält (eine Vor-Ort-Kontrolle kann so i.d.R. entfallen – bei beabsichtigter Vor-Ort-Kontrolle, ist dies im Arbeitsvertrag individuell zu vereinbaren)
- ☐ Dienstlichen E-Mails werden nicht an private E-Mail-Konten weitergeleitet
- ☐ Bei sensiblen Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern zu Hause/im Büro die Einsicht durch andere Mitarbeiterinnen und Mitarbeiter