Datenschutz – Home Office und virtuelle Konferenztools

Rechtssicher durchstarten!

IHK

Inhalt

Home Office und Mobiles Arbeiten

Home Office = Mitarbeiter arbeitet von Zuhause aus

Mobiles Arbeiten = Ortsunabhängiges Arbeiten

Organisationsverpflichtung
- Schulung
- Kontrollpflicht

Datenverarbeitung im Arbeitsverhältnis
→ Unternehmer trägt die datenschutzrechtliche Verantwortung
→ Dies gilt auch bei Home Office und Mobilem Arbeiten
→ Mitarbeiter dürfen personenbezogene Daten (pbD) ausschließlich auf Weisung des Verantwortlichen verarbeiten

Home Office und Mobiles Arbeiten

Arbeitgeber

- entscheidet über die datenschutzrechtliche Zulässigkeit
- Prüfkriterien – Einzelfallbezogen, d. h. differenzierte Prüfung nach
  - Art der Daten (sensibel, nicht sensibel)
  - Verwendungszwecke und –zusammenhänge
  - **Risiken** für Persönlichkeitsrechte Betroffener
    durch eingeschränkte Kontroll- und Einflussmöglichkeiten des Arbeitgebers

→ Risikominderung möglich?
→ Durch angemessene technische und organisatorische Maßnahmen
→ Durch Kontrollen

Home Office und Mobiles Arbeiten

Bewertung

- Schutzbedarf der pbD (normal, hoch, sehr hoch)
- Umstände und Risiken bei den Arbeitsabläufen

Praxistipp

- Vollständige medienbruchfreie Ausgestaltung (digital, nicht hybrid)
- Möglichst über betriebliche Arbeitsmittel und über verschlüsselte Kommunikationswege

Grundsatz
→ Daten sind um so mehr zu schützen, je sensibler und schutzbedürftiger diese sind.

Maßnahmen zum Schutz der Daten

- Schutz der Daten auf mobilen Geräten
  - → durch Verschlüsselung (Ende-zu-Ende-Verschlüsselung)
  - → Keine Anbindung von Druckern
  - → Sperrung von USB-Zugängen und anderen Anschlüssen
- Transport mobiler Geräte
  - → nur im gesperrten Zustand
  - → nie unbeaufsichtigt
  - → Datenträger verschlüsselt, Schriftdokumente im Behältnis
- Sichere Authentifizierung
  - → Zwei-Faktor-Authentifizierung
  - → Zugangsdaten getrennt vom Gerät aufbewahren
- Zugriff auf Unternehmensinfrastruktur
  - → Geschützt über VPN
  - → Verbot der Nutzung öffentlicher Netzwerkzugänge
- Mitarbeiterschulung
  - → Schutz von Bildschirm und Tastatur beim mobilen Nutzen;
  - → Berufliche Telefonate extern nur im geschützten Bereich
  - → Sicherer Umgang mit digitalen Geräten
  - → Richtiger Umgang mit Datenvorfällen
- Datenverarbeitung im Auftrag
  - → Kontrollrechte von Kunden (Auftraggebern) und von Aufsichtsbehörden hat ein Arbeitgeber zu gewährleisten.

Praxisempfehlungen – weitere Schutzmaßnahmen

- Verantwortlichkeiten im Umgang mit pbD umfassend regeln
  → Vertrag/Betriebsvereinbarung (auch Zutritt zur Wohnung für Kontrollen!)
- Arbeitsmittel/Dokumente zugriffssicher aufbewahren und vertraulich behandeln
- Verbot der Privatnutzung der vom Arbeitgeber gestellten IT-Ausstattung
- Verbot der Nutzung privater Hard- und Software für Home Office und Mobiles Arbeiten
  (Ausnahme: Berufliche und private Daten wären auf Privatgeräten mandantenkonform trennbar)
- Verbot der Umleitung beruflicher E-Mails auf private E-Mail-Postfächer
- Einsatz eines Mobile Device Managements

Arbeitgeber hat Kontrollpflicht – Kontrolle routinemäßig

Datenschutzhinweise

Generell gilt

- Datenschutzgesetze wie die DSGVO sind zu beachten
  → u. a. Grundsatz „privacy by design/default“

Praxistipp

- Berücksichtigen Sie dies bereits bei der Auswahl des Tools
  - Datenschutzvorgaben und Umsetzung
  - Sicherheitsaspekte und Umsetzung

Datenschutzvorüberlegungen

- Geschäftliche Nutzung des Tools erlaubt?
- Datenschutz durch Technik/-voreinstellung
- Zugang zur Konferenz durch Link + PIN
- Sicherer Übertragungsweg
- Ausdrückliche Zustimmung möglich für Bildschirmfreigabe/Aufzeichnungen
  - → Unbefugte Aufzeichnung von Gesprächen: strafrechtsrelevant (Verletzung der Vertraulichkeit des Wortes, § 201 StGB)
- Löschung der Gespräche/Aufzeichnungen
  - → Grundsätzlich bei Meetingsende
- Kein Profiling der Teilnehmer
  - → Wenn Profiling, dann deaktivierbar?
- Vertrag über Auftragsverarbeitung
- Dienst in Europa oder aus Drittland?
  - → Übermittlung pbD an ein Drittland?
  - → angemessene Garantie?
    - → z. B. Standardvertragsklausel, EU-US Privacy Shield
    - → Einwilligung - wirksam vereinbar? (ausreichend informativ?)

Datenschutz – Erforderlichkeitsprüfung

Prüfen Sie die Funktionen eines Konferenztools auf Erforderlichkeit

Zweckbindung

- Welcher Zweck: Wofür wird diese Funktion benötigt?
- Geeignetheit: Lässt sich der Zweck damit erreichen?
- Verhältnismäßigkeit: Gibt es ein milderes Mittel? (z. B. Kein Video, wenn Audio ausreichend ist)

Praxistipp

- Sind Schutzmaßnahmen zur Umsetzung ergriffen/möglich?
  - Technische Maßnahme (z. B. Zugangscode plus Link, gesondertes Passwort pro Meeting)
  - Organisatorische Maßnahme (z. B. Löschung nach Meetingsende, Zustimmung zur Bildübertragung)

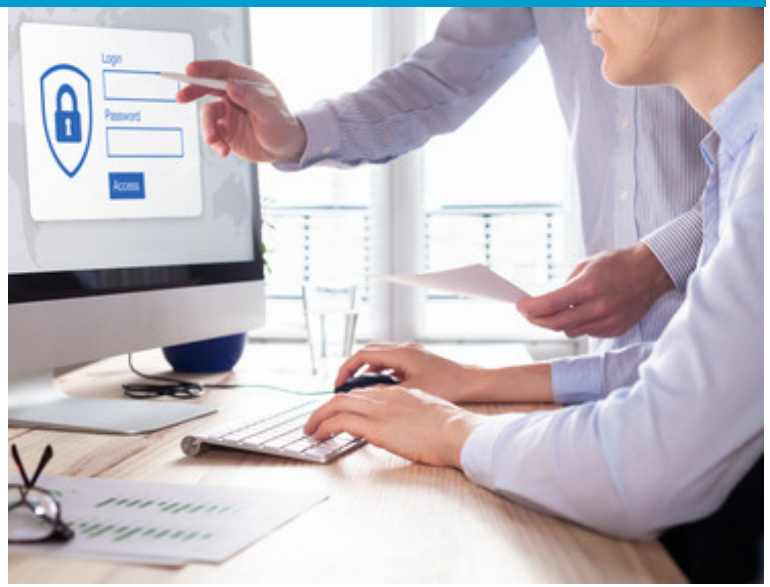
Datenschutz – allgemeine Vorgaben

- Verzeichnis von Verarbeitungstätigkeiten
- Informationspflicht
  - Art, Umfang und Zwecke der Verarbeitung, Rechtsgrundlage, Kategorien pbD / von Empfängern, Übermittlung an Drittland (angemessene Garantie!), Betroffenenrechte
  - Gegenüber Externen und Mitarbeitern
  - Gestaltungsoption: In der Datenschutzerklärung oder als gesonderte Informationspflicht
  - **Link** auf Informationspflichten in der Einladung zum Meeting

Sicherheitstipps für Videokonferenz-Apps

- Business-Version für Geschäftsmeetings
- Nutzen der „Wartezimmerfunktion“
  - → Moderator kann Teilnehmer im Warteraum aktiv zuschalten
  - → Absperren des virtuellen Meetingraums (alle TNer da)
  - → Moderator sollte Teilnehmer aktiv entfernen können
- Passwortschutz voreingestellt?
  - → Ansonsten stets einstellen (Datenschutzvoreinstellung)
  - → Sicheres Passwort verwenden
- Teilnehmer stets über die App einladen
  - → Nicht über Social Media
  - → Teilnehmer anweisen, Links nicht weiterzugeben oder zu teilen
- Einstellungsoptionen
  - → Bildschirmfreigabe nur durch Moderator, nicht durch TNer
  - → Teilnehmer bei Eintritt stumm schalten
  - → Neues Passwort pro Sitzung
  - → Deaktivierung der Funktion „Vor dem Gastgeber beitreten“
- Video-/Audiokonferenz
  - → Video nur, wenn Audio nicht ausreichend ist
  - → Funktion Teilnehmer-Video: Erst aktivieren bei TNergestattung
- Aktuell und upgedatet
  - → Aktuelle Softwareversion (Updates!) und Anti-Virensoftware
  - → Zwei-Faktor-Authentifizierung, falls keine Cloud-Lösung
  - → Verschlüsselung von Festplatten und Notebooks

Tipps und Infos – Home Office und Videokonferenz



IHK für München und Oberbayern

- https://www.ihk-muenchen.de/corona-homeoffice

DSK

- https://www.datenschutzkonferenz-online.de/entschliessungen.html
  Datenschutzgrundsätze bei der Bewältigung der Corona-Pandemie

Datenschutzaufsichtsbehörden

- https://www.lda.bayern.de/de/corona_datenschutz.html
- https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

BSI

- https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf
  Kompendium Videokonferenzsystem

Tipps und Infos – Home Office und Videokonferenz

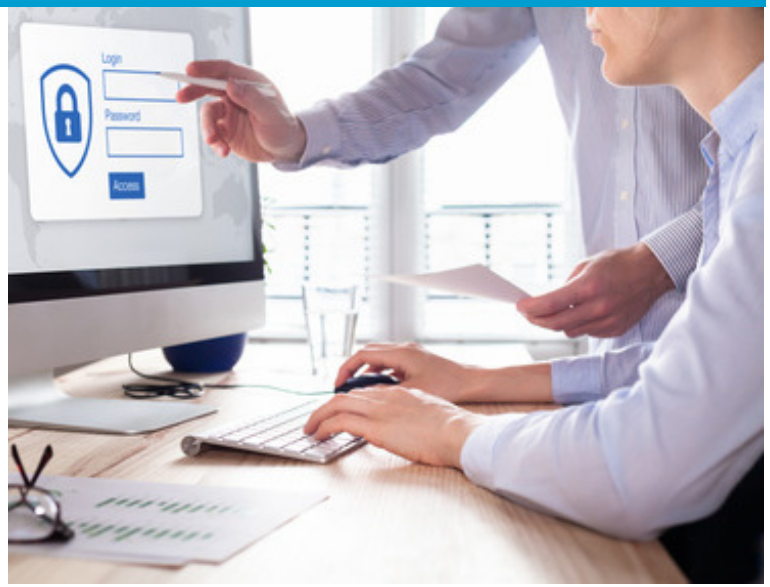
GDD

- https://www.gdd.de/aktuelles/startseite/neue-praxishilfe-videokonferenzen-und-datenschutz-erschienen
  - GDD-Praxishilfe DSGVO XVI „Videokonferenz und Datenschutz“
  - Anlage II - Übersicht über Videokonferenzsysteme, Messenger und Fernwartungssoftware

Weitere Links

(Suche z. B. „Videokonferenzsysteme DSGVO“)

- https://datenschutz-generator.de/dsgvo-video-konferenzen-online-meeting/
- https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/videokonferenz-und-datenschutz/
- https://www.datenschutzbeauftragter-info.de/videokonferenz-tools-tipps-zur-auswahl-und-verwendung/



Datenschutz – IHK-Ansprechpartner

Rita Bottler

Datenschutzbeauftragte der
IHK für München und Oberbayern
und des BIHK e. V.

rita.bottler@muenchen.ihk.de
dsb_bihk_ev@muenchen.ihk.de
089-5116-1683

Julia Franz

Referentin für Datenschutzrecht

franzj@muenchen.ihk.de
089-5116-2065

Fragen?