Paul Voigt
p.voigt@taylorwessing.com

Home Office & Datenschutz

Boris Johnson #StayHomeSaveLives
@BorisJohnson

This morning I chaired the first ever digital Cabinet.

Our message to the public is: stay at home, protect the NHS, save lives. #StayHomeSaveLives

♡ 21.100 15:52 - 31. März 2020

Paul Voigt
p.voigt@taylorwessing.com

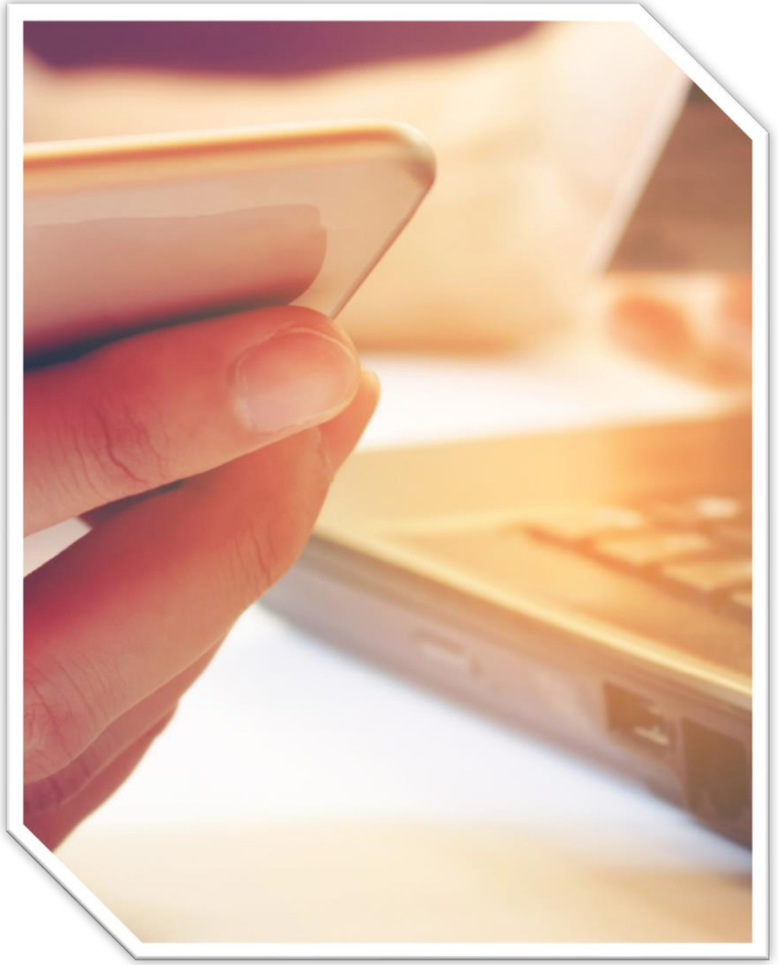
Home Office & Datenschutz

Grundsatz

- Arbeitgeber ist für die Sicherstellung der technischen und organisatorischen Maßnahmen verantwortlich (Art. 32 DSGVO)
- Klare Vorgaben für Arbeitnehmer / Sensibilisierung der Arbeitnehmer (Pflicht des Arbeitnehmer zur Sorgfalt); ggf. Datenschutzhinweise (Art. 13 DSGVO)
- Folgen bei Nichteinhaltung: Datenschutzverletzungen, ggf. auch andere Gesetzesverstöße

Erste Stellungnahmen von Datenschutz- und Sicherbehörden

- Bayerische Landesbeauftragte für den Datenschutz (öffentlicher Sektor / gültig bis 11.5.20)
- Ausnahmeweise Nutzung von Privatgeräten unter engen Voraussetzungen Unabhängiges Landeszentrum für Datenschutz (weitere Hinweise)
  - Home Office durch AVV (mit Kunden) ausgeschlossen?
  - Private Geräte: Datenspeicherung im verschlüsselten Bereich, unwiederbringliche Löschung (inkl. Löschung von Nummern bei automatischer Speicherung im Telefon)
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- European Union Agency for Cybersecurity (ENISA)

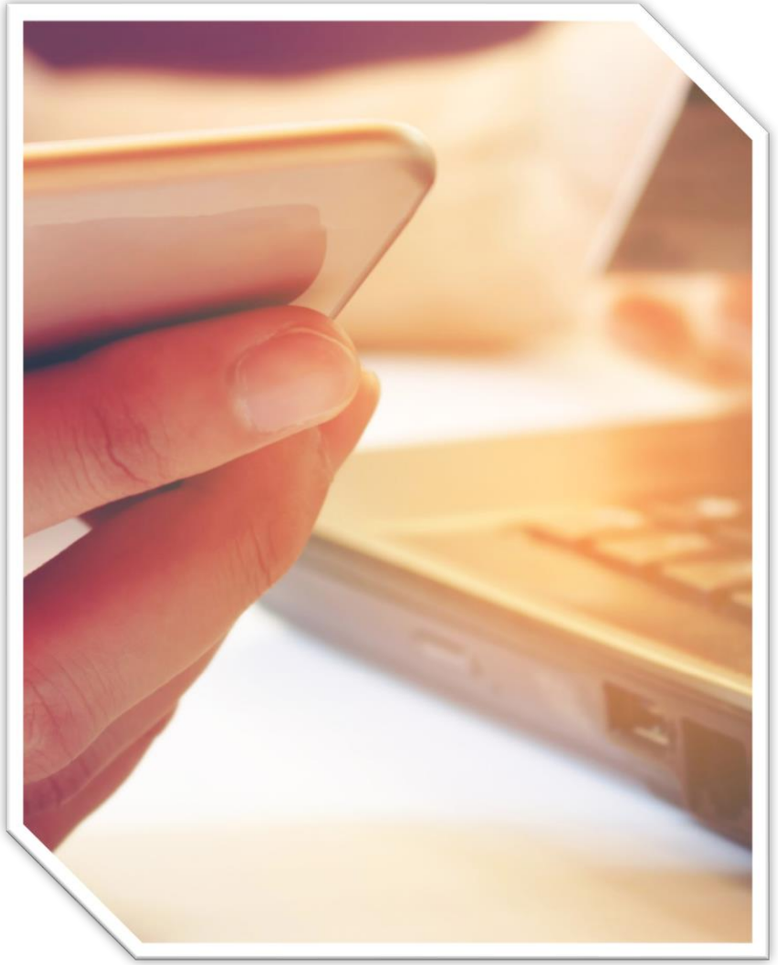


Paul Voigt
p.voigt@taylorwessing.com

Home Office & Datenschutz

Nutzung von Geräten des Arbeitgebers (Corporate Owned Devices)

- Zutritts- und Zugriffsschutz: Papierdokumente in verschließbaren Behältern (auf Minimum reduzieren), Papier, Laptop und Speichermedien wegschließen, abschließbarer Raum
- IT-Systeme: Härtung der IT-Systeme, Einspielen aktueller Software-Patches und aktueller Antivirenschutz sowie der Einsatz einer Firewall, Bildschirmschoner mit Passwortschutz, Verschlüsselung von tragbaren IT-Systemen und Datenträgern, Support durch IT
- Nutzung von Bildschirmfolien, min. nicht einsehbarer Bildschirm,
- Sicherer Remote-Zugriff auf das Netz der Institution (z.B. VPN), sichere Internetverbindung (verschlüsseltes WLAN oder Kabel)
- Datensicherung (Risiko der Beschädigung des Geräts: bestenfalls keine lokale Speicherung, Speicherung im System des AG)
- Kein Anschluss privater Geräte (z.B. Drucker, Bildschirme, USB-Sticks)
- Verlust / Offenlegung / sonstige Verstöße sofort melden! (z.B. wegen Art. 33 / 34 DSGVO)
- Entsorgung von vertraulichen Informationen (Datenschutz, Wirtschaftsspionage, etc.) nicht über den privaten Müll



Paul Voigt
p.voigt@taylorwessing.com

Home Office & Datenschutz

Nutzung von privaten Geräten (Bring your own Device)

- Soweit möglich, untersagen!
- Falls unumgänglich, sind folgende Maßnahmen zu ergreifen:
  - Bestenfalls nur zum Zugriff auf Unternehmensserver (Cloud)!
  - Arbeitgeber hat technische Voraussetzungen für die Verwendung privater Geräte zu schaffen: Trennung privater und dienstlicher Daten (z.B. Container-Lösung), Installation und Implementierung von IT-Sicherheitssystemen (z.B. Verschlüsselung, Firewall, Antivirenschutz, Passwortschutz), nur datensparsame Arbeiten
  - Sicherer Remote-Zugriff auf das Netz der Institution (z.B. VPN), sichere Internetverbindung (verschlüsseltes WLAN oder Kabel)
  - Unwiederbringliche Löschung von Daten
- Zudem: Kein Weiterleiten beruflicher E-Mails auf einen privaten E-Mail-Account
- Zudem: Nutzung von Software auf privaten Geräten?
  - Lizenzbestimmungen untersagen regelmäßig den gewerblichen Gebrauch.