

Checkliste für Unternehmen



Compliance-Support
für Ihr Team



1 Richtlinien aktuell halten

- BYOD-Regeln überprüfen und Hinweise für das Arbeiten im Homeoffice aufnehmen.
- Risiken von öffentlichem/privatem WLAN ansprechen und sichere Verbindungswege vorgeben.
- Richtlinien zum Drucken, Aufbewahren und Entsorgen von Papierdokumenten (Büro & Homeoffice) aktualisieren.
- Passwort-Richtlinien stärken (z.B. Drei-Wort-Passphrasen, MFA).
- Sichere Datenlöschung vor Entsorgung von IT-Geräten vorschreiben.

2 Regelmäßige Schulungen anbieten

- Mitarbeiter zu DSGVO-Grundlagen, Datenverarbeitung und den [sechs Grundprinzipien](#) schulen.
- Umgang mit sensiblen Papierdokumenten und Aufbewahrungsfristen in Richtlinie einbeziehen.
- Trainingsmodule mit Homeoffice-Sicherheit und neuen Richtlinien aktualisieren.
- Online-Trainingsportal nutzen, um Trainingsfortschritt & Fristen online zu verfolgen.
- Praktische Tools bereitstellen, z.B. Checkliste oder Selbsttest, wie z.B. Datensicherheits-Check.
- NIS2 Richtlinie in Schulungen als zusätzliche Cyber-Resilienz-Ebene erwähnen, besonders für IT- und Security-Teams.

3 Mitarbeiter richtig ausstatten

- Firmenlaptops bereitstellen statt private Geräte (BYOD) zu nutzen.
- In leistungsstarke Antivirus- und Firewall-Systeme investieren.
- Zugang zu Aktenvernichtern sicherstellen: Bürogeräte im Unternehmen, kompakte Geräte für das Homeoffice.
- Für die Entsorgung hochsensibler Dokumente Mikroschnitt Aktenvernichter (Sicherheitsstufe P-5) verwenden.
- Produktivität und Sicherheitsfunktionen priorisieren (z.B. Stauvermeidung, sichere Bedienung).

4 Klare und einheitliche Kommunikation

- Sicherheit auf allen Ebenen betonen; Wissenslücken bei neuen Mitarbeitern schließen.
- Datensicherheit in Live-Meetings, Team-Updates und 1:1-Gesprächen thematisieren.
- Richtlinien-Updates teilen, z.B. über Intranet, Newsletter und Aushänge.
- Phishing-/Cyberangriffs-Warnungen und Best Practices gezielt im Unternehmen kommunizieren.
- Datensicherheit fest in die Quartalsbesprechungen integrieren.
- DSGVO als zentrale Compliance-Grundlage positionieren und NIS2 gezielt ergänzen, wo sie die Cybersicherheitskultur stärkt.

Checkliste für Mitarbeitende



**Sicher fühlen
im Umgang
mit Daten**



1 Digitale Daten schützen

- Starke, individuelle Passwörter nutzen und in einem Passwort-Manager speichern.
- Zwei-Faktor-Authentifizierung aktivieren.
- Vorsicht vor Phishing · keine verdächtigen Links oder Anhänge anklicken.
- Geräte verschlüsseln, aktuell halten, mit Passwort schützen und Antivirus aktivieren.
- Bei Remote Arbeit das Unternehmens-VPN nutzen; öffentliches WLAN nur nach Freigabe.
- Unternehmensregeln bei Nutzung eigener Geräte (BYOD) beachten.

2 Sensible Papierdaten korrekt handhaben

- Sensible Daten erkennen: personenbezogene Daten, Geschäftsunterlagen, HR-Unterlagen, Finanzdokumente.
- Dokumente nach Ablauf der Aufbewahrungsfrist schreddern (z.B. Verträge, Personalakten Belege, Kontoauszüge).
- Vertrauliche Dokumente nicht offen liegen lassen – täglich Schreibtisch aufräumen und Unterlagen sicher verschließen.
- Druckbedarf prüfen – nur drucken, wenn wirklich nötig.
- Sensible Dokumente vor Entsorgung schreddern, niemals direkt ins Recycling geben.
- Gelagerte Dokumente regelmäßig prüfen und personenbezogene Daten, wenn möglich, anonymisieren.

3 Richtlinien einhalten und Schulungen wahrnehmen

- Schulungen und Auffrischungsmodule regelmäßig absolvieren.
- Risiken im Kollegenkreis verantwortungsvoll ansprechen.
- [Die sechs Grundprinzipien](#) des Datenschutzes kennen.
- Bei Unsicherheiten Rücksprache mit Vorgesetzten oder dem Datenschutzbeauftragten halten.
- Halten Sie sich über alle Änderungen der Unternehmensrichtlinien oder Datenschutzgesetze (einschließlich neuer Verordnungen wie NIS2) auf dem Laufenden.