Arbeitshilfe 1: Datenschutz-Kurzrichtlinie für neue Mitarbeiter

Diese Kurzrichtlinie ersetzt keine ausführlichen Richtliniensammlungen und Datenschutzhandbücher. Diese sind jedoch oft 50 Seiten und länger. Da verliert man schnell den Überblick. Deswegen gibt es zusätzlich diese Kurzform mit den allerwichtigsten Dingen rund um Datenschutz und KI.

1. Nutzung von Künstlicher Intelligenz (KI)

- Nur genehmigte KI-Systeme nutzen
- Keine privaten KI-Tools für dienstliche Zwecke einsetzen
- Keine sensiblen und personenbezogenen Daten eingeben
- Keine Betriebs- oder Geschäftsgeheimnisse eingeben
- KI-Training deaktivieren
- Bei Unsicherheit immer Rücksprache mit Datenschutzbeauftragtem (DSB) oder Datenschutzteam (DST) halten

2. Mobiles Arbeiten (Homeoffice, Außendienst etc.)

- Nur genehmigte Hard- und Software nutzen
- Daten grundsätzlich auf den zentralen Servern speichern, nicht auf lokalen Geräten
- Mobile Geräte verschlüsseln
- Keine privaten Geräte nutzen
- Arbeitsplatz auch zu Hause vor unbefugtem Zugriff schützen (z. B. Sichtschutz, Bildschirmsperre, Zugangskontrolle)
- Bei Verlust oder Diebstahl von Geräten sofort das DST informieren
- Auch beim mobilen Arbeiten gilt das Clean-Desk-Prinzip
- Keine vertraulichen Telefonate in öffentlicher Umgebung führen

3. Clean-Desk (Ordnung am Arbeitsplatz)

- Keine sensiblen Dokumente offen am Arbeitsplatz liegen lassen
- Papierunterlagen sicher verschließen, insbesondere nach Arbeitsende
- Bildschirme sperren, wenn der Arbeitsplatz verlassen wird
- In Meetingräumen keine sensiblen Daten offen sichtbar lassen

4. Umgang mit Betroffenenrechten (z. B. Auskunft, Löschung, Widerspruch)

- Jede Anfrage von Betroffenen sofort und vollständig an das DST weiterleiten
- Niemals selbstständig Auskünfte erteilen oder Daten löschen
- Identität des Anfragenden muss vor Herausgabe von Informationen geprüft werden.
- Reaktionszeit: unverzüglich. Spätestens innerhalb eines Monats muss das Unternehmen reagieren.

Arbeitshilfe 1: Datenschutz-Kurzrichtlinie für neue Mitarbeiter

5. Vorgehen bei einem Datenschutzvorfall

- Jeden Verdacht auf Datenverlust, Datenmissbrauch oder unbefugten Zugriff sofort dem DST melden
- Keine eigenen Untersuchungen starten oder Beweise verändern
- Frist: Innerhalb von 72 Stunden muss ggf. die Aufsichtsbehörde informiert werden.

Beispiele für einen Datenschutzvorfall:

- Ein unverschlüsseltes Notebook mit personenbezogenen Daten wird verloren oder gestohlen.
- USB-Sticks, externe Festplatten oder andere Datenträger mit unverschlüsselten Daten gehen verloren.
- Briefe oder Pakete mit personenbezogenen Daten kommen abhanden.
- Hacker dringen in IT-Systeme ein.
- Bei einem Einbruch werden personenbezogene Daten gestohlen.
- Zugangsdaten (Benutzername/Passwort) werden missbraucht, um Daten unbefugt zu verändern, zu kopieren oder zu löschen.
- Datenträger sind defekt, es gibt kein Back-up, die Daten sind endgültig verloren.
- Datenträger werden unsachgemäß entsorgt und sensible Daten gelangen in falsche Hände.

6. Löschfristen und Datenlöschung

- Daten dürfen nur so lange gespeichert werden, wie sie für den Zweck erforderlich sind.
- Löschfristen sind im Löschkonzept des Unternehmens geregelt.
- Keine eigenmächtige Löschung oder Archivierung auf privaten Speichermedien
- Löschanfragen nicht selbst bearbeiten, sondern an das DST weiterleiten