dsb
datenschutzbeauftragte
kanton zürich

Leitfaden

Regeln für das Homeoffice

Der Schutz und die Sicherheit der Daten stellt Mitarbeitende im Homeoffice vor besondere Herausforderungen. Die Berücksichtigung der folgenden Punkte erhöht die Sicherheit, insbesondere beim Einsatz von privaten Geräten oder wenn kein sicherer Zugang (Remote Access) auf Geschäftsinformationen zur Verfügung steht.

1 Updates installieren

Die Betriebssysteme und Programme auf PCs, Smartphones und Tablets sind immer auf dem aktuellen Stand zu halten. Deshalb soll regelmässig geprüft werden, ob Updates zur Verfügung stehen. Diese sind zu installieren. Mit Updates werden meist Sicherheitsschwachstellen behoben.

2 Starke Passwörter verwenden

Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Der Passwortcheck der Datenschutzbeauftragten hilft, ein starkes Passwort zu erstellen. Für jeden Dienst ist ein anderes Passwort zu verwenden. Die Passwörter können mit einem Passwortmanager verwaltet werden. Weitere Informationen im Merkblatt Passwortmanager.
Auch private Geräte wie Smartphones oder Notebooks, auf denen geschäftliche Informationen gespeichert werden, sind mit einem starken Passwort oder einer biometrischem Zugangssperre zu sichern. Wenn möglich ist eine Zwei-Faktor-Authentifizierung zu aktivieren (Benutzername, Passwort sowie ein weiterer Faktor, wie SMS, Secure ID).

3 Sichere Identifikation gewährleisten

Es dürfen sich nur Mitarbeitende selbst an Geräten anmelden. Passwörter dürfen nicht an Dritte weitergegeben werden.

4 Geschäftliche Informationen und Personendaten schützen

Geschäftliche Informationen und Personendaten sind auch im Homeoffice nach den Grundsätzen der Informationsverwaltung zu schützen:

- Interne Informationen und Personendaten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen.
- Der Bildschirm ist vor Einsicht zu schützen.
- Die Informationen sind sicher und geschützt zu speichern, beispielsweise auf einem verschlüsselten USB-Stick.
- USB-Sticks und andere Datenträger sind sicher aufzubewahren.
- Auf dem privaten Gerät sind Personendaten verschlüsselt und in einem eigenen Ordner zu speichern, getrennt von privaten Daten.
- Files oder Ordner können mit WinZip oder 7Zip verschlüsselt werden.
- Papierdossiers und Ausdrucke sind vor unberechtigtem Zugriff zu schützen.
- Nicht mehr benötigte Papierunterlagen sind zu schreddern respektive sicher aufzubewahren, bis sie im Büro vernichtet werden können.
- Nicht mehr benötigte Daten auf dem privaten Computer sind sicher zu löschen (nicht nur in den Papierkorb verschieben), sobald sie im Geschäftssystem abgelegt sind.

5 E-Mail sicher einsetzen

Private und geschäftliche E-Mails sind auf dem privaten Gerät zu trennen. Dazu können unterschiedliche Mail-Programme eingesetzt werden. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation ist zu vermeiden. Anhänge sind zu verschlüsseln und das Passwort ist separat auf einem zweiten Kommunikationsweg zu übermitteln. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.

6 Kommunikations-Tools gezielt auswählen

Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Der Kanton stellt seinen Mitarbeitenden die Videokonferenzlösung WebEx zur Verfügung. Informationen zu weiteren Diensten sind auf der Website der Datenschutzbeauftragten unter Digitale Zusammenarbeit zu finden.

7 Sich vor Phishing und anderen Bedrohungen schützen

Verdächtige E-Mails sollen nicht geöffnet werden. Anhänge in Mails von unbekannten Absendern sollen nicht angeklickt werden. Der geschäftliche IT-Support ist sofort zu informieren. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.

8 Datenverlust sofort melden

Wenn Arbeitsmittel wie Dokumente, Geräte oder USB-Sticks verloren gehen oder abhandenkommen, ist dies den Vorgesetzten respektive dem IT-Support sofort mitzuteilen.

Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich

- 5 Schritte für mehr Smartphone-Sicherheit
- E-Mail-Sicherheit
- Merkblatt Kommunikationssoftware
- Merkblatt Passwortmanager
- Leitfaden Einsatz mobiler Geräte in der Verwaltung
- Passwortcheck
- datenschutz.ch-App (enthält Passwortcheck, Smartphone-Lexikon etc.)

Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland)

- Merkblatt Tipps für sicheres mobiles Arbeiten

V 1.0 / April 2020

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh