Checkliste Datenschutz am Arbeitsplatz

Diözese Rottenburg-Stuttgart
Stabsstelle Datenschutz

Alle Mitarbeitenden tragen die Verantwortung für die datenschutzkonforme Ausübung ihrer Tätigkeit (§ 17 KDG-DVO). Wir empfehlen Ihnen, regelmäßig an Schulungsangeboten der Stabsstelle Datenschutz teilzunehmen. Um Ihnen über unser Schulungsangebot hinaus einen Überblick über die datenschutzrechtlichen Anforderungen am Arbeitspatz zu geben, haben wir nachfolgende Checkliste für Sie erstellt, die Ihnen zur Orientierung dienen kann. Die Checkliste hat ausdrücklich keinen Anspruch auf Vollständigkeit.

Arbeitsplatz

- ✓ An allen IT-Geräten ist der Passwortschutz zu aktivieren. Während der Arbeitszeit ist auch bei kurzzeitigem Verlassen des Arbeitsplatzes der Bildschirm (Windowstaste + L) manuell zu sperren. Ergänzend ist der Bildschirmschoner mit einem voreingestellten Intervall zu aktivieren, der im Falle einer vergessenen manuellen Sperre, den Bildschirm nach einem voreingestellten Zeitraum (i. d. R. 5 Minuten) automatisch sperrt.
- ✓ Bei Abwesenheit vom Arbeitsplatz muss man sich vom System abmelden und ggf. den PC abschalten.
- ✓ In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen werden kann. Bildschirmschutzfolien können dabei die Sicherheit unterstützen.
- ✓ Keine unbefugten Personen alleine im Büro zurücklassen.
- ✓ Im Grundsatz erfolgt keine Speicherung von personenbezogenen Daten ab Datenschutzklasse II auf mobilen Datenträgern. Erforderlichenfalls sind die Speichermedien zu verschlüsseln.
- ✓ Keine sensiblen Unterlagen bei eigener Abwesenheit offen auf dem Schreibtisch liegen lassen. Der Schreibtisch sollte vor dem Verlassen des Arbeitsplatzes, insbesondere vor dem Feierabend, aufgeräumt werden, so dass keine personenbezogenen Daten offen auf dem Tisch liegen bleiben. Akten und Datenträger (USB-Sticks, CDs, externe Festplatten und andere Speichermedien), die personenbezogene Daten beinhalten, sind in abschließbaren Räumen, Schränken, Behältern etc. aufzubewahren. Es ist dafür Sorge zu tragen, dass Unbefugte keine Einsicht in diese Akten und Datenträger nehmen können.
- ✓ Schriftstücke, die Personendaten oder vertrauliche Daten enthalten werden in geschlossenen Briefumschlägen verschickt.
- ✓ Ausdrucke direkt am Kopierer oder Drucker abholen.
- ✓ Bei Gesprächen ist die Vertraulichkeit zu gewährleisten: vermeiden Sie, dass unbefugte Dritte mithören können (z. B. bei Tür- und Angelgesprächen).
- ✓ Aktenvernichter mit geeigneter Schutzstufe gemäß DIN 66399 verwenden.
- ✓ Für Tätigkeiten im Homeoffice sind die speziellen Regelungen für mobiles Arbeiten zu beachten (https://datenschutz.drs.de/fileadmin/user_files/237/Dokumente/Aktuelles/Infoblatt_mobiles_Arbeiten_Datenschutz.pdf).

Schließverhalten

- ✓ Bürotüren bei eigener Abwesenheit immer abschließen.
- ✓ Zugangstüren und -tore außerhalb der Öffnungs- und Arbeitszeiten immer abschließen.
- ✓ Es ist eine Schlüsselliste zu führen, damit jederzeit nachvollziehbar ist, wer Zugang zum Gebäude oder zu Schränken hat.
- ✓ Bei Doppel- und Großraumbüros muss der/die Letztverlassende die ordnungsgemäße Schließung des Büros veranlassen.

Auskünfte per Telefon, E-Mail, Fax o. ä.

Telefonische Auskünfte

- ✓ Feststellung der Identität des Auskunftssuchenden.
- ✓ Abwesenheitsgründe von Mitarbeitenden nicht an Dritte kommunizieren.
- ✓ Es dürfen keine vertraulichen Nachrichten auf Anrufbeantworter gesprochen werden.

Mailverkehr

- ✓ E-Mails mit vertraulichem Inhalt und/oder personenbezogenen Daten dürfen nur über das diözesane Intranet (Secure-Mail-Gateway, S-Transfer) versandt werden, da hier eine geschützte und verschlüsselte Verbindung besteht.
- ✓ Der offen einsehbare E-Mail-Verteiler gehört zu den Klassikern unter den Verstößen gegen den Datenschutz, und das gleich aus zwei Gründen: Zum einen kann es Empfänger im Verteiler geben, die ihre E-Mail-Adresse grundsätzlich nicht öffentlich machen möchten. Zum anderen kann die E-Mail personenbezogene Daten enthalten, die auf keinen Fall ohne Zustimmung der betroffenen Person einer größeren Gruppe zugänglich gemacht werden sollen. (Zur Klarstellung: Bereits die E-Mail-Adresse selbst zählt zu den personenbezogenen Daten.)
  Daher sollte grundsätzlich durch Eintragung der E-Mail-Adressen in das „BCC-Feld“ (englisch: „Blind Carbon Copy“, dt. sinngemäß Blindkopie) die Übertragung der E-Mail-Adressen an die anderen Empfänger unterdrückt werden. Nur bei dienstlichen E-Mail-Adressen sowie bei rein sachbezogenen (= nicht personenbezogenen) Inhalten oder wenn die Adressaten in die Offenlegung ihrer E-Mail-Adresse eingewilligt haben, können die E-Mail-Adressen weiterer Empfänger in das „CC“-Feld eingetragen werden.
- ✓ Computerviren und andere Schadprogramme werden häufig über E-Mail-Anhänge verbreitet. Bei verdächtigen E-Mails darf daher auf keinen Fall der Anhang geöffnet oder ein enthaltener Link angeklickt werden, und bei einer suspekten E-Mail eines bekannten Absender muss nachgefragt werden, ob E-Mail und Anhang tatsächlich von dort abgeschickt worden sind.

Faxversand

Galt ein Telefax noch vor einigen Jahren als relativ sichere Methode, um sensible personenbezogene Daten zu übertragen, so hat sich diese Situation grundlegend geändert. Das „reine“ Faxgerät ist mittlerweile abgelöst. Meist handelt es sich um Multifunktionsgeräte mit Fax-Funktion oder Fax-Server. Eingehenden Faxe werden in E-Mails konvertiert und an ein E-Mail-Postfach weitergeleitet. Das "Faxgerät" könnte auch ein Fax-Dienst, wie zum Beispiel ein Cloud-Fax-Service sein, der als virtueller Fax-Server die Eingangsfaxe ebenfalls in E-Mails konvertiert und weiterleitet. Ob und gegebenenfalls wie die E-Mails dabei verschlüsselt sind, kann die sendende Stelle nicht feststellen. Hinsichtlich des Schutzziels Vertraulichkeit hat das Fax das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail.

Fax-Dienste enthalten in der Regel keinerlei Sicherungsmaßnahmen, um die Vertraulichkeit der Daten zu gewährleisten und sind daher in der Regel **nicht für die Übertragung personenbezogener Daten geeignet**.

Sollte in Ausnahmefällen ein Faxversand mit vertraulichem und/oder personenbezogenem Inhalt notwendig sein, ist ein konkreter Zeitpunkt der Übertragung mit der Gegenseite abzustimmen, damit das Fax unmittelbar nach Eingang von dem berechtigten Empfänger abgeholt und nicht von unbefugten Personen eingesehen werden kann.

Passwörter

- ✓ Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
- ✓ Das Speichern von Passwörtern im Browser ist nicht erlaubt.
- ✓ Passwörter müssen eine Mindestlänge von 8 Zeichen haben **und** aus einer Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen[1].
- ✓ Passwörter müssen komplex und nicht leicht zu erraten sein. Keine Vor- und Familiennamen, Geburtsdaten und keine Trivialpasswörter (z. B. 12345…)
- ✓ Einmal genutzte Passwörter können nicht wieder verwendet werden.
- ✓ Neue Mitarbeitende haben den Empfang von Initialpasswörtern bzw. voreingestellte Passwörtern zu bestätigen und müssen diese umgehend ändern.
- ✓ Das Passwort für den Zugriff auf das diözesane Intranet darf nicht gleichzeitig für Zugänge zu öffentlichen Webdiensten und für private Zwecke genutzt werden.

Stabsstelle Datenschutz
Stand 03/2022

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html