

DSGVO: Technische und Organisatorische Maßnahmen

Hinweis: Alle Angaben ohne Gewähr, es wird keine Haftung übernommen.

Artikel 32 DSGVO <https://dsgvo-gesetz.de/art-32-dsgvo>, „Sicherheit der Verarbeitung“ besagt:

„Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten,“

Die Maßnahmen umfassen:

- Pseudonymisierung und Verschlüsselung: z. B. Namen ausschwärzen, Festplatten oder Daten verschlüsseln
- Vertraulichkeit (z. B. unberechtigter Zugriff), Integrität (z. B. Backups), Verfügbarkeit (z. B. Ausfallsicherheit) und Belastbarkeit (z. B. genügend Ressourcen) sicherstellen
- Verfügbarkeit nach Zwischenfall rasch wiederherstellen (z. B. bei technischen Defekten)
- Regelmäßige Überprüfung, Bewertung und Evaluierung der Maßnahmen (z. B. testen, ob Backups korrekt einspielbar sind)

Beurteilung des Schutzniveaus:

- Risiken der Verarbeitung berücksichtigen
- Risiken von Vernichtung, Verlust, Veränderung ermitteln
- Risiken von unbeabsichtigter oder unrechtmäßiger Offenlegung ermitteln
- Risiken von unbefugte Offenlegung und unbefugtem Zugang ermitteln

Unterstelltes Personal verarbeitet Daten nur aufgrund einer Anweisung des Verantwortlichen.

Beachten Sie auch § 6 Datenschutzgesetz, „Datengeheimnis“:

<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597&FassungVom=2018-06-13>

Maßnahmenplan bei Anpassungsbedarf

Falls Sie nicht alle Maßnahmen rechtzeitig umsetzen können, sollten Sie die Umsetzung planen.

Gehen Sie wie folgt vor und dokumentieren Sie dies:

- Zeitliche und budgetäre Planung
- Maßnahmen festlegen
- Maßnahmen umsetzen

Beispiele für technische und organisatorische Maßnahmen

Ordnung: Weisen Sie alle Mitarbeiter an, Ordnung zu machen und zu halten. Die möglicherweise häufigste und offensichtlichste und einfach zu behebende Datenschutzverletzung sind offen liegende Dokumente mit personenbezogenen Daten, die von anderen einfach so gelesen werden können.

Mögliche organisatorische Maßnahme: Schreiben Sie ein Dokument „Allgemeine Bürorichtlinien“, das die einzuhaltende „Ordnung“ beschreibt.

Personen-Zutritt sichern: Stellen Sie sicher, dass die Unternehmensräumlichkeiten gesichert sind (versperrt, Alarmanlage, Portier, Empfang,...).

Frage: nur ein Mitarbeiter befindet sich im Moment im Unternehmen. Dieser geht auf das WC. Wie sind in diesem Fall die Räumlichkeiten gesichert?

Mögliche technische Maßnahme: Alarmanlage einrichten

Mögliche organisatorische Maßnahmen: Personal anweisen, Alarmanlage vor dem Verlassen aktivieren, Räumlichkeiten versperren falls niemand vom Personal anwesend ist,...

PC-Zutritt sichern: Stellen Sie sicher, dass PC-Arbeitsplätze gesichert sind (z. B. geeignete Passwörter).

Frage: ein Mitarbeiter verlässt den Arbeitsplatz. Wie ist in diesem Fall der Computer gesichert?

Mögliche technische Maßnahme: Windows-Taste + L zum schnellen Abmelden

Datensicherungen: Stellen Sie sicher, dass regelmäßig Daten gesichert werden. Testen Sie auch das „Wiedereinspielen“. Lagern Sie Datensicherungen an einem anderen Ort (z. B. Bankschließfach, anderes Gebäude), und auch offline.

Laptops, USB Sticks, Smartphones, Tablets mit personenbezogenen Daten: All diese Geräte sind insofern ein Sicherheitsrisiko, als diese leicht verloren gehen oder gestohlen werden können.

Mögliche technische Maßnahme: Daten am Gerät verschlüsseln, Zutritts-PIN

Mögliche organisatorische Maßnahmen: Keine personenbezogenen Daten auf solchen Geräten erlauben, Blickschutzfolie

Zugriffsstruktur: Stellen Sie sicher, dass je nach Personal nur auf jene personenbezogenen Daten zugegriffen werden kann, die für die Arbeit benötigt werden. Beispielsweise sollte ein Fahrlehrer nur Teile der personenbezogenen Daten von jenen Schülern sehen, die mit diesem die Fahrstunden fahren.

Mögliche technische Maßnahme: Zugriff auf Dateien und Ordner je nach Position sichern

Vernichtung von Daten: Stellen Sie sicher, dass bei Aktenvernichtung (Schülerakt nach mind. 7 Jahren Aufbewahrungspflicht) die Daten nicht in falsche Hände gelangen können. Papier in Altpapier ist kein Vernichten, eher ein Offenlegen. Übergeben Sie die Akten einem professionellen Aktenvernichtungsunternehmen, falls Sie keine andere sichere Vernichtung sicherstellen können.

Speichern Sie keine Passwörter: Ob im Browser, auf Smartphones, Tablets, oder auf Papier – geben Sie entsprechende Anweisungen, keine Passwörter zu speichern oder aufzuschreiben. Passwort-Manager sehen wir als nicht sicher an, da diese stets Ziel von Angriffen sein werden. Mögliche Ausnahme: auf Papier im Tresor, der nur der Geschäftsführung zugänglich ist – dies sollte ausreichend sicher sein. Sollten Sie Passwörter gespeichert haben, geben Sie die Anweisung diese zu vernichten und ändern Sie die Passwörter sicherheitshalber.

Löschen von Daten: Falls Sie einen Datenträger entsorgen möchten: Befanden sich auf einer Festplatte, einem USB Stick usw. Daten, reicht normales Löschen nicht aus. Auch hier gibt es entsprechende Datenvernichtungsunternehmen, falls keine andere Form der Vernichtung in Frage kommt.

Besonders nicht mehr funktionstüchtige Festplatten und USB Sticks stellen hier ein Problem dar: die Daten sind auf einfachem Wege nicht mehr verwendbar, auch jegliches „sichere“ Löschen per Software ist nicht möglich. Die Daten sind jedoch nicht verloren, Experten können die Daten wiederherstellen. Werfen Sie vermeintlich defekte Datenspeicher nicht einfach weg.