Fragenkatalog zu technischen und organisatorischen Maßnahmen zur Datensicherheit

1. Vertraulichkeit

Zutrittskontrolle

- Wie sind die Gebäude, in denen Daten verarbeitet werden, vor dem unberechtigten Zutritt geschützt?
- Gibt es eine Besucherregelung? Wenn ja, wie ist diese ausgestaltet?
- Gibt es eine Videoüberwachung?
- Sind sonstige Maßnahmen getroffen?

Zugangskontrolle

- Wie werden Berechtigungen zum Zugang zu Daten oder Systemen erteilt?
- Wird die Erteilung und der Entzug von Berechtigungen protokolliert? Wer hat Zugriff auf die Protokolle?
- Werden eingeräumte Berechtigungen periodisch im Hinblick auf ein weiteres Erfordernis überprüft? Wenn ja, wie häufig?
- Wie wird sichergestellt, dass nur erforderliche Berechtigungen eingeräumt werden?
- Gibt es eine Passwortrichtlinie?
- Welche Mindestpasswortlänge wird verlangt? Wird die Mindestlänge technisch erzwungen?
- Wird eine Passwortkomplexität verlangt? Wird diese technisch erzwungen?
- Wird ein Passwortwechsel erzwungen? Wenn ja, wann und wie?
- Werden externe Schnittstellen (z.B. USB) gesperrt?
- Werden mobile IT-Systeme verschlüsselt?
- Werden mobile Datenträger verschlüsselt?
- Wie werden IT-Systeme vor Viren und Schadsoftware geschützt?
- Wie werden unberechtigte Zugriffe von Dritten auf IT-Systeme erkannt und unterbunden?
- Wie wird Sorge dafür getragen, dass nur sorgfältig ausgewählte und überprüfte Dienstleister in Kontakt mit personenbezogenen Daten gelangen?

Zugriffskontrolle

- Wie wird gewährleistet, dass Berechtigungen differenziert vergeben werden?
- Werden Benutzerrollen und damit einhergehende Berechtigungen regelmäßig überprüft? Wenn ja, wie oft?
- Wie wird sichergestellt, dass Rechte von Personen beim Ausscheiden aus dem Unternehmen oder beim Wechsel einer Aufgabe im Unternehmen entzogen werden?
- Werden Zugriffe auf Anwendungen und/oder Daten protokolliert?
- Wie wird sichergestellt, dass nicht mehr verwendete Datenträger sicher gelöscht oder vernichtet werden?
- Wie wird sichergestellt, dass Papierunterlagen mit personenbezogenen Daten sicher vernichtet werden und die Vernichtung nachgewiesen wird?

Trennung

Wie wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten auch in getrennten Systemen verarbeitet werden?

Pseudonymisierung & Verschlüsselung

- Findet eine Pseudonymisierung oder Verschlüsselung von Daten statt? Wenn ja, bitte beschreiben.

2. Integrität

Eingabekontrolle

- Wie gewährleisten Sie, dass jederzeit festgestellt werden kann, *wer* personenbezogene Daten *wie* eingegeben, verändert oder gelöscht hat?
- Wie lange speichern Sie die Nachweise dieser Eingaben, Änderungen und Löschungen („Protokolle“)?
- Wer hat Zugriff auf diese Protokolle?

Weitergabekontrolle

- Wie werden personenbezogene Daten zwischen Auftraggeber und Auftragnehmer übertragen?
- Wie wird der Schutz der Daten während des Transports gewährleistet?
- Wie wird gewährleistet, dass Daten nach der Beendigung des Auftrags sicher gelöscht werden?
- Wie wird die Löschung dokumentiert?

3. Verfügbarkeit und Belastbarkeit

- Ist eine unterbrechungsfreie Stromversorgung (USV) für Serversysteme im Einsatz?
- Sind Serverräume klimatisiert?
- Gibt es Feuer- und Rauchmeldeanlagen? Bitte beschreiben.
- Ist eine Festplattenspiegelung im Einsatz? Wenn ja, welche?
- Bitte beschreiben Sie ihr Datensicherungs- und Wiederherstellungskonzept.
- Wo werden Datensicherungen aufbewahrt?
- Sind Datensicherungen verschlüsselt?
- Gibt es einen Notfallplan?
- Wie wird eine rasche Datenwiederherstellung gewährleistet?

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Hat die Unternehmensleitung Verantwortung für Datenschutz und Informationssicherheit übernommen („Leitlinie“)?
- Werden die Beschäftigten zum Datenschutz geschult? Wenn ja, wie und wie häufig? Gibt es Schulungsnachweise?
- Werden die Beschäftigten zum vertraulichem Umgang mit personenbezogenen Daten verpflichtet? Wie wird sichergestellt, dass alle Mitarbeiter zur Vertraulichkeit verpflichtet werden?

- Ist ein Datenschutzbeauftragter benannt worden?
- Welche Maßnahmen werden zur Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) getroffen?
- Gibt es Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten?
- Wie wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden?
- Gibt es einen Prozess zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA)?
- Wie wird sichergestellt, dass Anfragen von Betroffenen fristgemäß bearbeitet werden?
- Gibt es ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO?
- Welche Maßnahmen sind ansonsten getroffen worden, um die Umsetzung der Vorgaben der DSGVO im Unternehmen zu gewährleisten?
- Ist ein Datenschutzmanagementsystem (DSMS) implementiert worden?