Datenschutzaudit

Datenschutzaudit in Ihrem Unternehmen

- Das Audit als Anleitung zum Datenschutz in Ihrem Unternehmen
- Auditierung des Datenschutzkonzepts
- Audit der Verträge (Mitarbeiter, Auftragsverarbeiter, etc)
- Integration der Geschäftsleitung oder Ihres Datenschutzkoordnators

Ein Audit benötigt Zeit

Bitte gehen Sie davon aus, dass wir gemeinsam mit Ihnen oder Ihrem Datenschutzkoordinator für den gesamten Prozess je nach Größe des Unternehmens ein bis zwei Arbeitstage benötigen werden.
Nehmen Sie sich also ausreichend Zeit und stellen sie ggf. erforderliche Ressourcen und Prozesse zur Verfügung.

Datenschutzmanagementsystem

Zunächst sind die allgemeinen Pflichten, die die DSGVO an jeden Verantwortlichen stellt, zu überprüfen:

Datenschutzmanagement

- Existiert eine Datenschutzleitlinie bzw. Datenschutzhandbuch Datenschutzkonzept?
- Werden Löschfristen geregelt und umgesetzt?
- Wird die Nutzung der IT geregelt

Datenschutzorganisation

- Ist ein Datenschutzbeauftragter wirksam bestellt?
  Dessen Bestellung ist in der Regel ab zwanzig Mitarbeiter oder bei der Verarbeitung der besonderen Kategorie von personenbezogenen Daten notwendig.
- Sind weitere Aufgaben und Rollen im Rahmen des Datenschutzes verteilt?
- Wurde der Datenschutzbeauftragte der Behörde gemeldet und sind dessen Kontaktdaten intern sowie extern bekannt?

Datenschutzverletzungen (Art. 33 DSGVO)

- Bestehen Regelungen, Prozesse und Verantwortlichkeiten, wie bei einer Datenschutzverletzung zu handeln ist?

Anfragen Betroffener (Art. 15 ff. DSGVO)

- Bestehen Regelungen, Prozesse und Verantwortlichkeiten, wie mit Anfragen bzw. Anträgen Betroffener umzugehen ist.

Auftragsverarbeitung (Art. 28 DSGVO)

- Wurden alle notwendigen Auftragsverarbeitungsverträge geprüft und abgeschlossen? Ein solcher Vertrag ist dann notwendig, wenn ein anderes Unternehmen (auch im Konzern) Daten des Verantwortlichen in dessen Auftrag verarbeitet.
- Besteht ein Prozess zur datenschutzrechtlich konformen Einbindung externer Parteien?

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

- Besteht ein vollständiges Verzeichnis von Verarbeitungstätigkeiten? Der notwendige Inhalt wird in Art. 30 DSGVO bestimmt. Diese Informationen sind für jede Datenverarbeitung anzugeben.
- Ist dieses Verzeichnis als Nachweisdokument für die Behörde ausgestellt? Das Dokument dient laut DSGVO ausschließlich zur Information der Behörde. Es sollte daher aus sich heraus verständlich sein.

Datenschutzfolgenabschätzung (Art. 35 DSGVO)

- Wurden die Risiken der einzelnen Datenverarbeitungen evaluiert?
- Falls ein hohes Risiko für den Betroffenen besteht, wurde eine Datenschutzfolgenabschätzung durchgeführt?

Informationspflichten (Art. 13 f. DSGVO)

- Existieren Vorlagen zur Erfüllung der Informationspflichten
- Werden die Informationspflichten gegenüber Betroffenen erfüllt, bei denen Daten direkt erhoben wurden?
- Werden Daten von Dritten erhalten und werden in diesem Fall die Informationspflichten eingehalten?
- Existiert eine Datenschutzerklärung auf der Website?

Mitarbeiterschulung

- Werden Mitarbeiter ausreichend und regelmäßig auf den Datenschutz hin geschult? Der Arbeitgeber ist sonst für die Fehler seiner Mitarbeiter direkt verantwortlich.

Verpflichtung auf den Datenschutz

- Werden Mitarbeiter und externe Dienstleister vor dem ersten Kontakt mit personenbezogenen Daten auf die Einhaltung der Datenschutzvorschriften verpflichtet?

Informationssicherheit

Des Weiteren kann der Datenschutz im Unternehmen nur gelingen, wenn auch die Informationssicherheit beachtet wird. Der Datenschutz lebt von der technischen Umsetzung.

Pseudonymisierung und Verschlüsselung
(Art. 32 Abs. 1 lit. a DSGVO)

- Werden Daten nach Möglichkeit pseudonymisiert? Pseudonymisierung bedeutet, dass Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Achtung: Auch diese Daten unterliegen, anders als anonymisierte Daten, den Regelungen der DSGVO.
- Welche Geräte werden im Unternehmen verschlüsselt?
- Welche Verschlüsselungsart wird verwendet?

Vertraulichkeit
(Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Durch welche Maßnahmen wird das Unternehmen räumlich abgesichert?
- Zugangskontrolle: Wie werden die Datenverarbeitungssysteme vor dem Eindringen und der Nutzung Unbefugter gesichert?
- Zugriffskontrolle: Wie wird verhindert, dass personenbezogene Daten außerhalb der eingeräumten Berechtigungen verarbeitet werden können
- Trennungskontrolle: Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, auch getrennt verarbeitet werden?

Integrität
(Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle: Welche Versendungsart (digital und physisch) besteht beim Versand von Daten an Kunden, Auftraggeber bzw. Dritte und wie wird diese geschützt?
- Eingabekontrolle: Ist die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege gewährleistet?

Verfügbarkeit und Belastbarkeit
(Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle: Sind die Systeme so eingerichtet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind?
- Belastbarkeitskontrolle: Besitzen die Systeme die Fähigkeit, mit risikobedingten Veränderungen umgehen zu können und weisen sie eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen auf?

Wiederherstellbarkeit
(Art. 32 Abs. 1 lit. c DSGVO)

- Existiert ein Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall?

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Incident-Response-Prozess: Ist ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen implementiert?
- Datenschutzfreundliche Voreinstellungen: Werden die möglichen Voreinstellungen in Datenverarbeitungssystemen so getroffen, dass nur Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind und werden diese möglichst kurz gespeichert?
- Regelmäßige Überprüfungen: Werden die technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit hin evaluiert?

Verarbeitungstätigkeiten

- Zuletzt sind die speziellen Datenverarbeitungsvorgänge im Unternehmen zu durchleuchten, ob diese den datenschutzrechtlichen Vorgaben der DSGVO entsprechen. In diesem Bereich sind konkrete Vorgaben schwierig, da kein Unternehmen dem anderen gleicht und sich individuelle Problemstellungen ergeben.