Checkliste „Technische und organisatorische Maßnahmen (TOM)“ gemäß Art. 32 Abs. 1 DS-GVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Prüffokus:

Welche technischen bzw. organisatorischen Maßnahmen werden zur Zutrittskontrolle eingesetzt?

- Lage der Räume:
  Sind die Zugänge der Räume ausreichend abgesichert (z. B. Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben, Feuerleiter, Feuertreppe, elektrische Türöffner)?

- Verschließbarkeit der Räume:
  Gibt es ein geregeltes Konzept zur Schlüsselverwaltung?
  Findet eine Quittierung bei der Schlüsselausgabe statt?
  Wer besitzt einen Generalschlüssel?

- Schriftliche Festlegungen zur Zugangsberechtigung:
  Wer darf die Räume betreten?

- Reinigungs- und Wartungsarbeiten:
  Ist sichergestellt, dass sowohl mit dem Reinigungspersonal als auch mit IT-Dienstleistern bei Wartungen entsprechende Regelungen getroffen sind?

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Prüffokus:

Welche Maßnahmen sind hinsichtlich der Benutzeridentifikation und Authentisierung technisch und organisatorisch vorhanden?

- Firewall und Virenschutz:
  Welche Produkte werden eingesetzt?
  Existiert eine zentrale Firewall?
  Welche dezentralen Lösungen werden an den Arbeitsplätzen verwendet?

- Benutzeridentifikation und Passwortverfahren:
  Werden ausreichend sichere Passwörter verwendet (z. B. Sonderzeichen verwenden, empfohlene Länge)?
  Ist ein regelmäßiger Passwortwechsel verpflichtend?
  Findet eine Auswertung der Protokolleinträge bei Falscheingaben des Passworts statt?

- Systemsperrung:
  Erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen?
  Findet ein Sperren eines Zugangs bei mehr als drei Anmelde-Fehlversuchen statt?
  Hat die Falscheingabe eines Passworts eine zeitliche Verzögerung für einen Neuversuch zur Folge?

- Benutzerkennungen:
  Wird auf Gruppenkennungen verzichtet?
  Besteht ein eigenes Benutzerkonto für jeden Mitarbeiter?

- Verschlüsselung:
  Werden mobile Datenträger verschlüsselt?
  Welche Verschlüsselungsverfahren kommen zum Einsatz?

- Geräteanschlüsse:
  Sind an den relevanten PCs die USB-Steckplätze bzw. DVD/CD-Laufwerke gesperrt, um einen unbefugten Datentransport zu verhindern?

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Prüffokus:
Welche Maßnahmen sind vorhanden, um die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern?

- Berechtigungskonzept und Zugriffsrechte:
  Entspricht das Konzept sowohl für Anwender als auch für Administratoren den aufgabenbedingten und datenschutzrechtlichen Erfordernissen?
  Existieren differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung und Löschung?

- Schutz gegen unberechtigte Zugriffe:
  Bestehen Schutzmaßnahmen gegen unbefugte interne und externe Zugriffe (z. B. durch Verschlüsselung, Firewalls)?
  Werden Verfahren zur Data Leak Prevention (Erkennung unerwünschter Datenabflüsse) eingesetzt?
  Werden regelmäßig Penetrationstests gegen Attacken von Hackern durchgeführt?

- Überwachung und Protokollierung:
  Werden Zugriffe bzw. Zugriffsversuche protokolliert?
  Wann findet eine Auswertung der Protokolle statt?
  Wo und wie lange werden die Protokolle aufbewahrt?

- Datenträgerverwaltung:
  Sind die Datenträger inventarisiert (Art und Anzahl)?
  Wird die Lagerung von Datenträgern überprüft (dauernd/zeitweise, Bestandsverzeichnisse)?
  Werden Nachweise über Eingang, Ausgang sowie Bestand von Datenträgern festgehalten?

Wo werden die Datenträger, insbesondere mobile wie USBFestplatten, nach Dienstschluss aufbewahrt (abschließbare Schränke, Schlüsselregelung)?
Findet eine Auslagerung von Sicherungsdatenträgern statt?

- Datentrennung:
  Findet eine äußerliche Kennzeichnung der eigenen Datenträger zur Unterscheidung von fremden statt?
  Besteht eine Regelung zum Einsatz privater Datenträger?

- Datenlöschung:
  Werden Datenträger vor neuer Verwendung vollständig von bestehenden Daten bereinigt?
  Werden Daten auf den Datenträger vor Weitergabe gelöscht?

- Entsorgung/Vernichtung:
  Werden auch Fehldrucke sorgfältig entsorgt?
  Werden veraltete Datenträgern geregelt vernichtet (entsprechende Lagerung der zu vernichtenden Datenträger, Datenträgerlöschgeräte, Verbrennen/Zerstören)?
  Finden Kontrollen der tatsächlichen Vernichtung bei Dienstleistern statt (zuverlässiges Entsorgungsunternehmen, vertragliche Regelung, Entsorgungsbescheinigung)?
  Welche Schredder werden eingesetzt (Sicherheitsstufe)?

- Regelung für das Kopieren von Datenträgern:
  Existieren Richtlinien für das Kopieren von Datensätzen bzw. auch für das vollständige Kopieren von Datenträgern?

- Regelungen für mobile Geräte:
  Gibt es Anweisungen zum Umgang mit mobilen Datenträgern und Geräte (z. B. USB-Sticks, externe Festplatten, Tablets, Smartphones)?
  Wird BYOD (Bring-Your-Own-Device) in der Organisation gelebt?

- Fernwartung:
  Bestehen Regelungen und gezielte Kontrollen bei Wartungsarbeiten durch Dienstleister (externe Wartung und Fernwartung)?

Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Prüffokus:
Wie wird gewährleistet, dass Daten getrennt voneinander verarbeitet werden können?

- Getrennte Speicherung:
  Welche Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung existieren? Wie erfolgt die Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Zwecken (z. B. getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke)?
  Wie werden Daten mit hohem Schutzbedarf verarbeitet?

- Mandantenfähigkeit:
  Werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung)?

Besteht ein Konzept zur Mandantentrennung

- Funktionstrennung:
  Werden Produktion- und Testumgebungen stets voneinander getrennt?
  Werden personenbezogene Daten zu Entwicklungszwecken pseudonymisiert/anonymisiert?

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Prüffokus:
Welche Regelungen existieren bezüglich der Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle)?

- Datenträgertransportart:
  Welche unterschiedlichen Datenträgertransporte finden statt (z. B. nur innerhalb des Verantwortlichen, zur Auslagerung, zwischen Auftraggeber/-nehmer, zu Dritten)?

- Versendungsarten:
  Wie werden die Daten versendet (z. B. Post, Kuriere, elektronisch)?

- Transportregelungen:
  Ist definiert, welche Personen die Datenträger befugt entnehmen dürfen?
  Werden beim Transport Datenträgerbegleitpapiere ausgestellt bzw. mitgenutzt?
  Existiert eine verbindliche Regelung, wer als Datenempfänger fungieren darf und wer zur Weitergabe berechtigt ist?

- Transportsicherung:
  Sind die Datenträger beim Transport ausreichend gesichert?
  Werden durchgängig sichere Versendungsformen verwendet (z. B. Wertpaket, Einschreibesendung, Datentransport-/E-Mail-Verschlüsselung, elektronische Signatur, VPN/Virtual Private Network)?
  Werden elektronische Datentransporte Ende-zu-Ende verschlüsselt?

- Dokumentation:
  Werden die Abruf- und Übermittlungsvorgänge dokumentiert?
  Wird der Eingang und Ausgang von Datenträgern schriftlich festgehalten?
  Gibt es Legitimation der Abholer, Empfangsbestätigungen, Ein-/Ausgangsbücher, Protokollierung?

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Prüffokus:
Welche Maßnahmen werden insbesondere zur Protokollierung bei Änderungen in den Datenverarbeitungssystemen ergriffen?

- Protokollierung:
  Welche Protokollierungs- und Protokollauswertungssysteme kommen zum Einsatz?
  Was wird im Rahmen der Protokollierung aufgezeichnet (z. B. wer erfasst, wer hat wann was eingegeben)?
  Werden auch Online-Eingaben bzw. Änderungen sorgfältig protokolliert?
  Welche Regelungen zur Aufbewahrungsdauer der Protokolle bestehen?

3. Verfügbarkeit und Belastbarkeit der Systeme sowie deren Wiederherstellung (Art. 32 Abs. 1 lit. b, c DS-GVO)

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Prüffokus:
Welche Regelungen bestehen, um die Daten dauerhaft verfügbar bereitzustellen?

- Brandschutz:
  Welche Einrichtungen zum Brandschutz sind vorhanden (z. B. Feuerlöscher, Rauch- oder Brandmelder)?
  Besteht Rauchverbot?

- Sicherungen:
  Werden Sicherungsdatenträger getrennt aufbewahrt?
  Wo erfolgen die Backup-Verfahren?
  Werden Speichereinheiten redundant ausgelegt?
  Sind die Datensicherungen verschlüsselt?
  Werden Cloud-Lösungen zur Datensicherung eingesetzt?

- Virenschutz/Firewall:
  Bestehen ausreichende Schutzmaßnahmen durch Security-Werkzeuge?

- Notfallplan:
  Gibt es auch für einen Katastrophenfall entsprechende Vorkehrungen (z. B. durch Angriffe von intern/extern, Schäden durch Feuer)?

4. Maßnahmen im Rahmen der Datenverarbeitung im Auftrag gemäß Art. 28 DS-GVO

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Prüffokus:
Welche Regelungen bestehen im Umgang mit Auftragsverarbeitern?

- Auswahl von Auftragnehmer:
  Findet Auswahl der Auftragnehmer sorgfältig statt?

- Unterauftragnehmer:
  Ist das geprüfte Unternehmen selbst als Auftragnehmer tätig?
  Welche Auftragnehmer werden dort nach welchen Kriterien ausgewählt?

- Schriftliches Auftragsverhältnis:
  Bestehen detaillierte schriftliche Regelungen der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes - auch zum Einsatz von Subunternehmen (Erfassung, Scannen, Entsorgung)?
  Gibt es eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Datenträgertransport)?
  Erfolgt eine formalisierte Auftragserteilung (Auftragsformular)?

- Kontrolle:
  Findet eine regelmäßige Kontrolle der Arbeitsergebnisse statt (formal, inhaltlich)?
  Erfolgt auch eine Kontrolle der Unterauftragnehmer (z. B. durch den DSB)?

5. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

Verschlüsselung: Vorgang, bei dem klar lesbare Informationen (Klartext) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine nicht einfach interpretierbare Zeichenfolge (Geheimtexte) umgewandelt werden.

Sofern diese Maßnahmen für die Verarbeitungstätigkeit erforderlich sind, sind diese im Einzelfall zu treffen bzw. in den Nummern 1 bis 4 enthalten.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

Die Überprüfung, welche Maßnahmen zur Gewährleistung der Datensicherheit umgesetzt werden und ob, diese bezogen auf das prognostizierte Risiko geeignet sind, ein angemessenes Schutzniveau zu gewährleisten, hat in regelmäßigen Abständen zu erfolgen.