Self-Audit Datenschutz / DSGVO
Checkliste

1. Fragen an die Geschäftsleistung / den Verantwortlichen

a. Haben Sie sich schon mit den neuen Anforderungen der DSGVO und des BDSG (neu) befasst? Kennen Sie insbesondere die neuen Regelungen

- zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung? (Art. 5 Absatz 2 DSGVO)

  Ja □/ Nein □

- zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten? (Art. 12 - 14 DSGVO)

  Ja □ / Nein □

- zu den Rechten der Betroffenen auf Datenübertragbarkeit (Art. 20 DSGVO)?

  Ja □ / Nein □

- zur technischen und organisatorischen Sicherheit der Datenverarbeitung Art. 32 DSGVO?

  Ja □ / Nein □

- zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO)?

  Ja □ / Nein □

- zur Meldung von Datenschutzverstößen (Art. 33 DSGVO)?

  Ja □ / Nein □

b. Wurde ein interner/externer Datenschutzbeauftragter bestellt (Art. 37 DSGVO, § 38 BDSG neu)?

   Ja □ / Nein □

c. Wurden die Mitarbeiter zu den neuen Regelungen Bereich Datenschutz informiert? Ja □ / Nein □

d. Gibt es regelmäßige Schulungen für Mitarbeiter / Beschäftigte? Ja □ / Nein □

2. Bestandsaufnahme

a. Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 I DSGVO)?

- Verarbeitung von Kundendaten
- Verarbeitung von Beschäftigtendaten
- Verarbeitung von Daten von Kindern
- etc.

b. Wird dieses Verzeichnis regelmäßig aktualisiert? Ja □ / Nein □

c. Sind Sie Auftragsverarbeiter? Ja □ / Nein □ - Falls ja, führen Sie ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 II DSGVO? Ja □ / Nein □

3. Zulässigkeit der Verarbeitung

Sie benötigen auch nach neuem Recht für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

a. Haben Sie für alle Verarbeitungen eine Rechtsgrundlage (Art. 6 bis 11 DSGVO sowie § 26 BDSG neu)?

b. Haben Sie dies dokumentiert? Ja □ / Nein □

c. Haben Sie Ihre Einwilligungserklärungen an die Anforderungen von Art. 7 und 13 DSGVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

   Ja □ / Nein □

4. Betroffenenrechte und Informationspflichten

a. Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DSGVO). Wie stellen Sie alle in Art. 13 und 14 DSGVO genannten Punkte sicher?

- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
- Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer
- Hinweis auf Betroffenenrechte
- Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Wider-ruf der Einwilligung
- Recht auf Beschwerde bei der Aufsichtsbehörde
- Herkunft der Daten

b. Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15-22 DSGVO)?

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf fristgemäße Löschung der verarbeiteten Daten
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

5. Daten von Kindern

a. Verarbeiten Sie auch personenbezogene Daten von Kindern in Bezug auf Dienste der Informationsgesellschaft3?

b. Wenn ja, haben Sie in diesen Fällen an die besonderen Anforderungen an die Einwilligung gedacht (Art. 8 DSGVO)?

6. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

a. Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DSGVO)? Ja □ / Nein □

b. Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung dokumentiert? Ja □ / Nein □

c. Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? In welchen Fällen? Ja □ / Nein □

d. Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept? Ja □ / Nein □

e. Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Art. 25 DSGVO)? Ja □ / Nein □

7. Verträge

a. Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d.h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 26 – 28 DSGVO) angepasst? Ja □ / Nein □

b. Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben? Ja □ / Nein □

c. Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist, entsprechende zusätzliche Garantien/Vereinbarungen? Ja □ / Nein □

- EU-Standardvertragsklauseln Ja □ / Nein □
- Binding Corporate Rules Ja □ / Nein □
- Privacy Shield (nur für die USA) Ja □ / Nein □

8. Datenschutz-Folgenabschätzung (DSFA)

a. Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Art. 35 DSGVO)? (z.B. bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten) Ja □ / Nein □

b. Falls ja, haben Sie für die in diesen Fällen erforderliche DSFA in Ihrem Unternehmen einen Prozess eingeführt?

   Ja □ / Nein □

c. Wer ist für diesen Prozess zuständig?

9. Meldepflicht

a. Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DSGVO)? Ja □ / Nein □

b. Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet? Ja □ / Nein □

c. Wer ist in Ihrem Unternehmen für die Meldung zuständig?

d. Falls Sie einen Datenschutzbeauftragten bestellt haben, haben Sie bereits die Meldung seiner/ihrer Kontaktdaten an die Aufsichtsbehörde vorgenommen? Ja □ / Nein □

10. Dokumentation

a. Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen?

   Ja □ / Nein □

b. Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?