Check-Liste für Unternehmen zur Umsetzung der Datenschutz-Grundverordnung (DS-GVO)

(unverbindlich)

A: Struktur und Verantwortlichkeit im Unternehmen

1. Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch
   - Vorhandensein einer Datenschutzleitlinie
   - Beschreibung der Datenschutzziele
   - Regelung der Verantwortlichkeiten
   - Bewusstsein über Datenschutzrisiken
   - Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)

2. Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?

   - Wenn nein, warum nicht?
   - Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?
   - Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?

B: Übersicht über Verarbeitungen

1. Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO erstellt?
   - Wenn nein, warum nicht?
   - Ist das dokumentiert?

2. Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design – Art. 25 DS-GVO)?

C: Einbindung Externer

1. Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?
   - Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?
   - Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

D: Transparenz Informationspflichten und Sicherstellung der Betroffenenrechte

1. Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?
   - Wenn nein, warum nicht?

2. Haben Sie insbesondere folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:

   - Kontaktdaten des Datenschutzbeauftragten
   - Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
   - Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die berechtigten Interessen
   - Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln)
   - Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer
   - Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität
   - Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung
   - Recht auf Beschwerde bei der Aufsichtsbehörde
   - Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
   - Sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie – in diesem Fall – Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person
   - Sofern Sie die Daten nicht bei der betroffenen Person erhoben haben: aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen
   - Haben Sie Ihre Werbe-Einwilligungserklärungen für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

3. Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?

4. Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?

E: Verantwortlichkeit, Umgang mit Risiken

1.1. Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z.B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)?

1.2. Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 DS-GVO entsprechen?

1.3. Können Sie das Vorliegen der Einwilligung nachweisen?

2. Haben Sie einen Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?

3.1. Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?

3.2. Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?

3.3. Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?

3.4. Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?

4.1. Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?

4.2. Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt?

4.3. Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden? Haben Sie diesen schon einmal getestet?

F: Datenschutzverletzungen

1. Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist?

2. Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können? Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrem Unternehmen eingeführt?

3. Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist?

4. Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?