Checkliste zur Umsetzung der DSGVO

QaSiDa
Qualität Sicherheit Datenschutz

Ab dem 25. Mai 2018 muss jedes Unternehmen die Vorgaben der DSGVO und des neuen Bundesdatenschutzgesetzes (BDSG neu) umsetzen und in den Unternehmensalltag integrieren. Die folgenden Fragen helfen, die Bereiche in Ihrem Unternehmen zu identifizieren, in denen Sie schon gut vorbereitet sind und die Bereiche, in denen noch Handlungsbedarf für Sie besteht.

Erläuterung:

☑ **JA (wir setzen dies bereits um)** ☒ **NEIN (wir setzten dies noch nicht um)**

1. Verzeichnis von Verarbeitungstätigkeiten

Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DSGVO)? Denken Sie hierbei insbesondere an die:

☐ Verarbeitung von Kundendaten

☐ Verarbeitung von Beschäftigtendaten

☐ Verarbeitung von Daten von Kindern

☐ Verarbeitung von Daten für Dritte als Auftragsverarbeiter

2. Zulässigkeit der Verarbeitung

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

☐ Haben Sie für alle Verarbeitungen eine Rechtsgrundlage nach der neuen Rechtslage (Art. 6 bis 11 DSGVO sowie § 26 BDSG neu)?

☐ Haben Sie dies dokumentiert?

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

3. Betroffenenrechte und Informationspflichten

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 diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DSGVO genannten Punkte sicher? *(z.B. als Informationsschreiben oder in der Datenschutzerklärung auf Ihrer Webseite*)

Besonders wichtig sind in diesem Zusammenhang folgende Informationen:

☐ 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 Widerruf der Einwilligung
- ☐ Recht auf Beschwerde bei der Aufsichtsbehörde
- ☐ Herkunft der Daten

Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15-22 DSGVO)? Denken Sie dabei insbesondere an folgende Rechte:

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

4. Personenbezogene Daten von Kindern (*sofern eine Verarbeitung erfolgt*)

Verarbeiten Sie auch personenbezogene Daten von Kindern in Bezug auf Dienste der Informationsgesellschaft?

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

5. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

- ☐ Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung dokumentiert?
- ☐ Haben Sie Ihre Mitarbeiter auf das Datengeheimnis verpflichtet?
- ☐ Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein?
- ☐ Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?
- ☐ Ist sichergestellt, dass bei der Beschaffung von IT, Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mitberücksichtigt werden (Art. 25 DSGVO)?

6. Verträge prüfen

☐ 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? Dokumentieren Sie auch Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

☐ Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist, entsprechende zusätzliche Garantien/Vereinbarungen?

- EU-Standardvertragsklauseln
- Binding Corporate Rules

7. Datenschutz-Folgenabschätzung

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

☐ Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?

☐ Haben Sie einen Zuständigen für diesen Prozess benannt?

8. Meldepflichten

☐ Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DSGVO)?

☐ Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet?

☐ Haben Sie in Ihrem Unternehmen einen Zuständigen für die Meldung benannt?

☐ Falls Sie einen Datenschutzbeauftragten bestellt haben, ist die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde bereits erfolgt?

9. Dokumentation

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

☐ Können Sie sicherstellen, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

Haben Sie Handlungsbedarf festgestellt oder sind Sie sich in manchen Punkten unsicher? Gerne unterstützen wir Sie dabei den Datenschutz in Ihrem Unternehmen rechtsicher umzusetzen oder prüfen Ihr bereits bestehendes Datenschutzkonzept.

Kontakt:
Heinrichstraße 64 / 36043 Fulda
Büro: 0661/ 382255
Mobil: 0151/44880085
Email: info@qasida.de

QaSiDa
Qualität Sicherheit Datenschutz