Industrie- und Handelskammer zu Düsseldorf
Postfachadresse: Postfach 10 10 17 · 40001 Düsseldorf
Hausadresse: Ernst-Schneider-Platz 1 · 40212 Düsseldorf
Telefon 02 11 35 57-0

Checkliste DSGVO

Die folgende Checkliste soll Ihnen helfen herauszufinden, ob die DSGVO auf Ihr Unternehmen anwendbar ist (1. Kasten), sowie welche Folgen die Anwendbarkeit nach sich zieht (2. Kasten). Die Checkliste stellt eine überblicksartige Zusammenfassung dar und erhebt deshalb keinen Anspruch auf Vollständigkeit. Weitere Informationen der IHK Düsseldorf zum Thema Datenschutz finden Sie hier.

✓ Personenbezogene Daten

Alle Einzelangaben über persönliche und sachliche Verhältnisse, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (weites Verständnis; z.B. Name, IP-Adresse, Standort, E-Mail-Adresse, Alter, Geschlecht; nicht aber anonymisierte Daten).

✓ Datenverarbeitung

Jede(r) mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang / Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (z.B. Erheben, Erfassen, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Abgleichen, Löschen oder Vernichten, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung).

✓ Marktortprinzip

Datenverarbeitung von in der EU befindlichen Personen.

✓ Unzulässigkeit der Datenverarbeitung, sofern kein Erlaubnistatbestand greift (Art. 6 Abs. 1 DSGVO)

- → Einwilligung (freiwillige, umfassend informierte und eindeutige Zustimmung zu der Datenverarbeitung)
- → Bestehendes oder geplantes Vertragsverhältnis (Datenverarbeitung ist für die Vertragserfüllung notwendig)
- → Rechtliche Pflicht
- → Lebenswichtige Belange (Für den Schutz von Leib und Leben, z.B. in einem Krankenhaus oder auf einer Gesundheitskarte)
- → Wahrnehmung einer Aufgabe im öffentlichen Interesse
- → Berechtigtes Interesse an der Datenverarbeitung (Interessenabwägung)

Zur Klärung des einschlägigen Erlaubnistatbestandes ist daher zu prüfen, zu welchem Zweck die Daten verwendet werden (Zweckbindung der Datenverarbeitung). Insbesondere ist das Vorliegen von ausreichenden Einwilligungen zu überprüfen und diese sind ggf. erneut einzuholen.

✓ Datenschutzfreundliche Grundeinstellungen

Technische Systeme und die Grund- bzw. Voreinstellungen der Website müssen – im Lichte der Grundsätze der Datenvermeidung und Datensparsamkeit – datenschutzfreundlich ausgestaltet sein („Privacy by Design“ und „Privacy by Default“, z.B. durch Pseudonymisierung).

✓ Informationspflicht des Verarbeiters (Art. 13, 14 DSGVO)

Transparenz in präziser, verständlicher, leicht zugänglicher Form sowie in einer klaren und einfachen Sprache.

Notwendig ist daher insbesondere eine Anpassung der Datenschutzerklärung (d.h. umfassende Informationen zu dem Umgang mit Daten in Verbindung mit z.B. Kontaktformularen, Newslettern, Webanalyse- und Tracking-Tools, Cookies, Social-Plug-Ins, der Weitergabe der Daten an Dritte, Internetmarketing, Zahlarten, der Dauer der Speicherung, der Rechte der Betroffenen, mit Name und Kontaktdaten des für die Datenerhebung Verantwortlichen und des Datenschutzbeauftragten).

✓ Betroffenenrechte (Art. 15 ff. DSGVO)

Recht der betroffenen Person gegen den für die Datenverarbeitung Verantwortlichen auf Auskunft, Berichtigung, Löschung oder Sperrung, Datenübertragung, Widerspruch, Widerruf der Einwilligung, Beschwerderecht bei der Datenschutzaufsichtsbehörde sowie das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.

D.h. es müssen personelle und finanzielle Ressourcen vorliegen, die dazu geeignet sind, das Datenschutzverfahren einzuhalten (z.B. das Vorliegen eines Löschkonzepts, die Schulung der Angestellten oder Benutzung von datenschutzrechtkonformen Systemen).

✓ Verpflichtung auf Datengeheimnis sämtlicher Mitarbeiter

✓ Ggf. Datenschutz-Folgenabschätzung

In Fällen, in denen durch die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht sowie in besonders sensiblen Fällen im Sinne des § 35 DSGVO bzw. gemäß der Einschätzung der Aufsichtsbehörde ist eine Datenschutz-Folgenabschätzung durchzuführen.

✓ Verarbeitungsverzeichnis anlegen

Verzeichnis über alle Verarbeitungstätigkeiten gemäß Art. 30 DSGVO (ausgenommen können in bestimmen Fällen Kleinunternehmen mit unter 250 Mitarbeitern sein).

✓ Ggf. Datenschutzbeauftragten benennen

Bestellung eines unabhängigen und nicht-weisungsgebunden Beauftragten (intern oder extern) ist unter bestimmten Voraussetzungen zwingend (§ 38 BDSG 2018). Weitere Informationen finden Sie hier.

✓ Ggf. Beachtung der Vorschriften zur Auftragsverarbeitung (Art. 28 DSGVO)

Ggf. Anpassung der vertraglichen Vereinbarungen notwendig. Auftragnehmer muss Datenschutz auf dem Niveau der DSGVO bieten.

✓ Rechtsfolgen von Verstößen

→ Mitteilungspflicht von Verletzungen an die Aufsichtsbehörde (Art. 33 DSGVO) bzw. Beschwerderecht der betroffenen Person.
→ Sanktionen in Form von Bußgeldern sollen abschreckende Wirkung haben und können auch bei erstmaligem oder fahrlässigem Verstoß mit geringer Intensität auferlegt werden (Art. 84 DSGVO).
→ Daneben Haftung für etwaige materielle und immaterielle Schäden.