



Industrie- und Handelskammer
Bonn/Rhein-Sieg



**Der Countdown läuft! – EU-Datenschutz-
Grundverordnung jetzt umsetzen!**

Die EU-Datenschutz-Grundverordnung (DSGVO) gilt ab dem 25.05.2018.

Sie betrifft de facto jedes Unternehmen unabhängig wie groß oder klein es ist.

Die Verordnung schreibt den Datenschutz nicht ganz neu.

Sie verlangt jedoch umfangreiche Dokumentations- und Aufklärungspflichten.

Dies bedeutet, dass der Unternehmer nachweisen muss, dass er die Vorgaben der DSGVO einhält. Dazu bedarf es eines geeigneten Managementsystems.

Bei Verstößen gegen die Vorgaben der DSGVO droht ein Bußgeld von bis zu 20 Mio. Euro oder bis zu 4 % des weltweiten Jahresumsatzes .

Was ist zu tun?

Pflichten der Verantwortlichen:

engl.: **Accountability = Haftung**

Art. 5 DS-GVO:

Die Verarbeitung personenbezogener Daten

- muss rechtmäßig, nach Treu und Glauben und transparent erfolgen
- darf nur für den festgelegten, legitimen Zweck erfolgen
- ist auf das notwendige Minimum zu beschränken
- darf nur mit korrekten Daten erfolgen; Berichtigung/Löschung
- muss Löschfristen beachten, wenn Zweck erreicht

UND

Der Verantwortliche muss dies nachweisen können!

= sog. **Rechenschaftspflicht!!** (Art. 5 Abs. 2 DS-GVO)

Rechenschaftspflicht gem. Art 5 Abs. 2 DS-GVO

Wie kann ich meiner Rechenschaftspflicht genügen?

oder

Was bedeutet die Rechenschaftspflicht?

Ich muss wissen, welche Daten wie im Unternehmen verarbeitet werden.

Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherstellen zu können.

Art. 30 DSGVO Verzeichnis von Verarbeitungstätigkeiten

(1) **Jeder Verantwortliche** und gegebenenfalls sein Vertreter **führen ein Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- a. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- b. die Zwecke der Verarbeitung;
- c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- d. die Kategorien von Empfängern, gegenüber denen die personenbezogenen

Rechenschaftspflicht gem. Art 5 Abs. 2 DS-GVO:

Neben: Rechtmäßigkeit, Transparenz, Zweckbindung,
Datenminimierung, Richtigkeit, Lösungsverpflichtung

muss gewährleistet sein,

- dass technische und organisatorische Maßnahmen (=TOM) für einen angemessenen Schutz vor unbefugtem Zugriff, unbeabsichtigtem Verlust, Zerstörung, getroffen wurden (Art 24 DS-GVO)
- Ggfls. Einwilligung der Betroffenen vorliegt (Art 7 DS-GVO)
- Ggfls. Datenschutzfolgenabschätzung (Art 35 DS-GVO)

Rechenschaftspflicht gem. Art 5 Abs. 2 DS-GVO:

Benötigt wird

- ein Konzept des Datenschutzes durch Technikgestaltung (Art. 25 DS-GVO) **= Privacy by Design**
- sowie Datenschutzfreundliche Voreinstellungen

= Privacy by Default

z.B.: Benötigen wir das Kundengeburtsdatum für ein Angebot/Rechnung ?

- ein Datenschutzkonzept **= Data Strategy**
 - Aufbau einer Prozesskette
 - Datenschutzfolgeabschätzung
 - Berücksichtigung der Betroffenenrechte

Rechtmäßigkeit der Verarbeitung personenbezogener Daten

- Gesetzlich zulässig, rechtmäßig
 - Zur Erfüllung eines Vertrages (Art. 6 DS-GVO)
 - Erstellung eines Angebots (Art. 6 DS-GVO)
 - Wahrung berechtigter Interessen, z.B. Werbung (Art. 6 DS-GVO)
(Werbung per E-Mail erfordert eine Einwilligung)

ABER nur, wenn formelle Anforderungen erfüllt (Art. 12 bis 22 DS-GVO)

- **Informationspflichten:**
 - Angabe der Rechtsgrundlagen
 - Kontaktdaten des Verantwortlichen
 - Zweck und Erforderlichkeit der Datenerhebung
 - Dauer der Speicherung und Löschung
 - Widerrufsrecht
 - Beschwerderecht

Betroffener macht seine Rechte geltend

- Auskunft
- Löschung
- Berichtigung
- Übertragung

Notwendig hierzu:

Konzepte, Datenschutz-Management-Systeme

In der Schublade muss Handlungsanweisung liegen!

Eine **Auskunft** ist innerhalb von **einem Monat** zu erteilen

Eine Verletzung des Schutzes personenbezogener Daten, ist unverzüglich, spätestens aber innerhalb von **72 Stunden** der Aufsichtsbehörde (LDI NRW, Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Frau Helga Block, Düsseldorf) zu melden.

und

bei einem voraussichtlich hohem Risiko für den Betroffenen ist dies entspr. Art 34 DS-GVO zudem unverzüglich „in klarer und einfacher Sprache“ dem Betroffenen mitzuteilen.

Ihre Aufgabenstellung:

- Verzeichnis aller Verarbeitungstätigkeiten (Art. 30 DS-GVO)
 - Zweck -> Rechtsgrundlage - Art 6 DS-GVO
 - Betroffene -> Information DS-Erklärung
 - Datenkategorien
 - Datenquelle
 - Aufbewahrungsfristen
 - Löschfristen / Löschkonzepte
 - Empfängerkategorie
 - Auftragsverarbeiter
 - Mittel der Verarbeitung -> TOM
- Information ggü Betroffenen bei Datenerhebung (Muster 1)
- Betroffenenrechte -> Konzepte
- Mitarbeiterschulung -> Verpflichtungserklärung

Angebote Ihrer IHK Bonn/Rhein-Sieg:

Merkblätter zum Download unter www.ihk-bonn.de Webcode 76

Info-Veranstaltungen am

02.05.2018, 15.00 - ca 17.30 Uhr Webcode 6492158

07.05.2018, 16.30 - ca. 19.00 Uhr Webcode 6492159

Teilnehmerentgelt 25 €

Anmeldung online unter www.ihk-bonn.de

Fragen zur DSGVO ?

Detlev Langer Tel. 0228 2284-134 Mail: langner@bonn.ihk.de

Vanessa Schmeier Tel. 0228 2284-237 Mail: schmeier@bonn.ihk.de