Handwerkskammer
Ostwestfalen-Lippe zu Bielefeld

Vorgehen Datenschutz (EU DSGVO)

Folgende Schritte sind notwendig:

1. Bestandsaufnahme

a) Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten1 verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)2? Denken Sie hierbei insbesondere an die
- **Verarbeitung von Kundendaten**
- **Verarbeitung von Beschäftigtendaten**
- **Verarbeitung von Daten von Kindern**
- **Verarbeitung von Daten für Dritte als Auftragsverarbeiter**

b) Wird dieses Verzeichnis regelmäßig aktualisiert?
Wer ist hierfür in Ihrem Unternehmen zuständig?

2. Zulässigkeit der Verarbeitung

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

a) Haben Sie für alle Verarbeitungen (s.o. Nr. 2) eine Rechtsgrundlage nach der neuen Rechtslage (Art. 6 bis 11 DS-GVO sowie § 26 BDSG neu)?

b) Haben Sie dieses dokumentiert?

c) Haben Sie Ihre Muster für 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. Betroffenenrechte und Informationspflichten

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

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 Wider-ruf der Einwilligung**
- **Recht auf Beschwerde bei der Aufsichtsbehörde**
- **Herkunft der Daten**

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

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

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

5. 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 DS-GVO)? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung dokumentiert?

b) Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein?
In welchen Fällen?

c) Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?

d) Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Art. 25 DS-GVO)?

6. Verträge prüfen

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 DS-GVO) angepasst?

Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

b) Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland5 möglich ist, entsprechende zusätzliche Garantien/ Vereinbarungen?

- **EU-Standardvertragsklauseln**
- **Binding Corporate Rules**
- **Privacy Shield (nur für die USA)**

7. Datenschutz-Folgenabschätzung

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

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

c) Wer ist für diesen Prozess zuständig?

8. Meldepflichten

a) Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)?

- **Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet?**
- **Wer ist in Ihrem Unternehmen für die Meldung zuständig?**

b) Falls Sie einen Datenschutzbeauftragten bestellt haben, denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde.

9. Dokumentation

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

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