Fragenkatalog Querschnittsprüfung DS-GVO

1. Vorbereitung auf die DS-GVO

Wie haben Sie sich als Unternehmen auf die DS-GVO vorbereitet?

Schildern Sie (kurz) die Vorgehensweise, welche Bereiche involviert waren und welche Maßnahmen initiiert wurden. Sofern noch nicht alle Maßnahmen vollständig umgesetzt wurden, erläutern Sie bitte auch den Umsetzungsstatus.

2. Verzeichnis von Verarbeitungstätigkeiten

Wie haben Sie sichergestellt, dass alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen wurden? Wie stellen Sie dessen Aktualität sicher? Legen Sie bitte eine Übersicht Ihrer dokumentierten Verfahren sowie ein Beispielverfahren als Muster bei.

3. Zulässigkeit der Verarbeitung

Auf Basis welcher Rechtsgrundlagen verarbeiten Sie personenbezogene Daten? Sofern Sie auch auf Basis von Einwilligungen personenbezogene Daten verarbeiten, legen Sie bitte Ihre verwendeten Muster bei.

4. Betroffenenrechte

Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher? Skizzieren Sie Ihre diesbezüglichen Prozesse und gehen Sie insbesondere detailliert darauf ein, wie Sie Ihren Informationspflichten nachkommen. Vorhandene Musterinformationen fügen Sie bitte bei.

5. technischer Datenschutz

a. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?

b. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen an den jeweiligen Stand der Technik angepasst werden?

c. Wie stellen Sie sicher, dass Sie für die von Ihnen aktuell oder zukünftig eingesetzten IT-Anwendungen ein dokumentiertes datenschutzkonformes Rollen- und Berechtigungskonzept haben?

d. Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Privacy by Design und by Default)?

6. Datenschutz-Folgenabschätzung

a. Wie stellen Sie sicher, dass Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen erkannt und für diese eine Datenschutz-Folgenabschätzung durchgeführt wird?

b. Haben Sie in Ihrem Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen identifiziert? Welche?

Fügen Sie bitte die jeweilige Dokumentation zur Datenschutz-Folgenabschätzung bei.

7. **Auftragsverarbeitung**

   Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DS-GVO angepasst? Sofern Sie Musterverträge verwenden, fügen Sie diese bitte bei, darüber hinaus fügen Sie bitte einen aktuellen Beispielvertrag mit einem Ihrer Auftragsverarbeiter bei.

8. **Datenschutzbeauftragter**

   Wie ist Ihr Datenschutzbeauftragter in Ihre Organisation eingebunden? Welche Fachkundenachweise hat er?

9. **Meldepflichten**

   Wie stellen Sie sicher, dass Ihr Unternehmen Datenschutzverstöße fristgemäß an die Aufsichtsbehörde meldet? Skizzieren Sie Ihre diesbezüglichen Prozesse.

10. **Dokumentation**

    Wie können Sie die Einhaltung aller vorstehend in Ziff. 2 – 9 genannten Pflichten nachweisen?