Datenschutz-Grundverordnung

ÖSTERREICHISCHER FLIESENVERBAND

Die Datenschutz-Grundverordnung tritt am 25. Mai 2018 in Kraft. Bis dahin müssen alle Maßnahmen nach den neuen gesetzlichen Regelungen umgesetzt sein.

Checkliste zur Überprüfung der Maßnahmen

Überprüfen Sie Ihren Ist-Zustand, um auf dieser Basis die weiteren Anpassungs- und Umsetzungsschritte zu definieren:

Welche personenbezogenen Daten werden in Ihrem Unternehmen verarbeitet? (z.B. Name, Adresse, Geburtsdatum, Bankdaten aber auch IP-Adresse der Website-User etc.)

Welche Datenanwendungen bestehen in Ihrem Unternehmen?

- Welche Standardanwendungen liegen derzeit vor? (z.B. Rechnungswesen und Logistik, Mitgliederverwaltung, Kundenbetreuung und Marketing für eigene Zwecke etc.)
- Sind derzeit Datenanwendungen im Datenverarbeitungsregister registriert? Wenn ja, welche?
- Wird eine Bildverarbeitung durchgeführt? (z.B. Videoüberwachung)
- Erfolgt Profiling (automatisierte Erstellung von Profilen)?

Auf Basis welcher Rechtsgrundlage erfolgt die Datenverarbeitung? (z.B. Vertragserfüllung, rechtliche Pflichten, Einwilligung etc.)

Zu welchen Zwecken erfolgen die Datenverarbeitungen? (z.B. Werbezwecke etc.)

Werden sensible Daten verarbeitet? Wenn ja, welche? (z.B. Gesundheit, Religion, politische Meinung etc.)

Werden Kindern Dienste der Informationsgesellschaft angeboten (z.B. Webshop) und die erforderliche Einwilligung durch den Obsorgeberechtigten eingeholt?

Werden Auftragsverarbeiter (Dienstleister) zur Datenverarbeitung herangezogen?

- Gibt es schriftliche Vereinbarungen für die Auftragsdatenverarbeitung?
- Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?

Werden die Informationspflichten erfüllt und bereitgestellt?

Werden die Betroffenenrechte erfüllt und bereitgestellt?

- An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?

Wurden Ihre Geschäftsunterlagen in Hinblick auf die Datenanwendungen und die Verarbeitung personenbezogener Daten überprüft und überarbeitet? (z.B. AGB, Datenschutzerklärungen, Impressum, laufenden Verträge, Website-Einstellungen etc.)

Welche Maßnahmen sind für die Datensicherheit vorhanden und sind diese ausreichend?

Wie sind „privacy by design“ (Grundsätze des Datenschutzes durch Technik) und „privacy by

Datenschutz-Grundverordnung

ÖSTERREICHISCHER FLIESENVERBAND

default" (datenschutzfreundliche Voreinstellungen) implementiert?

Bestehen für Ihre Datenverarbeitungen Dokumentationspflichten? (Verzeichnis von Verarbeitungstätigkeiten)

- Wie wird die Dokumentationspflicht erfüllt?

Welche Vorkehrungen gegen Datenschutzverletzungen existieren in Ihrem Unternehmen?

Ist für die Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen?

- Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und Freiheiten der Betroffenen?
- Wie kann der Risikoeintritt verhindert oder zumindest minimiert werden?

Ist eine vorherige Konsultation bei der Aufsichtsbehörde notwendig? (bei hohem Risiko für die Rechte und Freiheiten der betroffenen Person und wenn keine Maßnahmen zur Eindämmung des Risikos getroffen werden können)

Benötigt ihr Unternehmen einen Datenschutzbeauftragten? (bei Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, z.B. Banken, Versicherungen etc., sowie bei Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten, z.B. Krankenanstalten etc.)

Besteht Datenverkehr mit dem EU-Ausland? Wenn ja, auf Basis welcher Rechtsgrundlage?

Wurden die Besonderheiten im Arbeitnehmerdatenschutz überprüft?

- Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen etc.
- Kommunikation und Abstimmung mit dem Betriebsrat

Wie weisen Sie nach, dass Ihre Datenverarbeitungen DSGVO-konform erfolgen? („Pflichten des Verantwortlichen" und „Grundsätze und Rechtmäßigkeit der Verarbeitung"; z.B. Dokumentation der Einwilligungserklärungen, Verarbeitungsverzeichnis, Dokumentation der ergriffenen Sicherheitsmaßnahmen, Dokumentation der Risikoabschätzung, Protokollierung oder Dokumentation der Weisungen an dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen, Dokumentation der Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit etc.)

Rechtsdurchsetzung und Strafen: Rechtsbehelfe, Haftungen und Sanktionen

Bei schwerwiegenden Verstößen können Geldbußen von bis zu € 20 Mio. oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

Verträge und Formularvorlagen finden Sie auf www.wko.at
Stand: Mai 2018; Quelle: www.wko.at