DS-GVO Checkliste

Die DS-GVO Compliance Checkliste beinhaltet die Voraussetzungen, die die neue europäische Datenschutz-Grundverordnung mit 25.05.2018 einführt. Hier werden die wichtigsten Bestimmungen zusammengefasst und auf die DS-GVO verwiesen. Diese Checkliste ist nicht abschließend zu verstehen und ersetzt selbstverständlich keine individuelle rechtliche Beratung.

A) Datenschutz-Bestandsaufnahme („Inventur“);
B) Umsetzung der DS-GVO;
C) Laufender Betrieb,

ad A) Zur Datenschutzinventur

Teamaufstellung

□ Mitarbeiter aus den Bereichen IT, Recht und Organisation;

Datenschutzinventur

□ Prüfen, welche pers.bez. Daten verarbeitet werden;
□ Prüfen, wie pers.bez. Daten bislang verarbeitet werden;

Infrastruktur

□ Prüfung zum Ist-Zustand der Infrastruktur (Schutz der technischen Anlagen, Trennungsgebot, Eingabekontrolle, Passwortschutz, Safe, …);
□ Prüfung zum Ist-Zustand der Software;

Maßnahmen

□ Erstellung eines Maßnahmenkatalogs (siehe ad B);

ad B) Zur Umsetzung der DS-GVO:

Rechenschaftspflicht

□ Einführung einer Datenschutzstrategie, die Vorgehensweisen und technische und organisatorische Maßnahmen (TOM's) und eine entsprechende Dokumentation der eingeführten Maßnahmen vorsieht:

□ Compliance bei Vertraulichkeit;

Art. 5, 24, 25, 30 DS-GVO;

Unternehmensführung und Kontrolle

□ Prüfung, ob ein Datenschutzbeauftragter notwendig ist;

□ Prüfung, ob eine zu benennende Person als Datenschutzbeauftragter ausreichend qualifiziert ist;

□ Überprüfung der Versicherungsdeckung und ob diese im Lichte der neuen Regelungen und Strafausmaße anzupassen ist;

□ Schulung der Mitarbeiter in Datenschutzangelegenheiten;

Art. 5, 27, 37-39 DS-GVO;

Einwilligung und rechtmäßige Verarbeitung

□ Überprüfe die gesetzliche Basis der Datenverarbeitung. Entspricht diese den Anforderungen der DS-GVO?

□ Werden sensible personenbezogene Daten verarbeitet? Sicherstellen, dass die gesetzlichen Anforderungen an die Datenverarbeitungen gewährleistet sind;

□ Überprüfe die bestehenden Einwilligungen, ob diese den Anforderungen der DS-GVO gerecht werden. Falls nicht, sind Abläufe zu definieren, damit hinsichtlich der bestehenden Datensätze neue Einwilligungen eingeholt werden;

Art. 5, 6, 7, 9, 10, 85- 91 DS-GVO;

Personenbezogene Rechte und Abläufe

□ Anpassung der Datenschutzerklärung und der internen Abläufe bei Anfragen;

□ Sicherstellen der technischen und operationalen Prozesse, zur Umsetzung der personenbezogenen Rechte, beispielsweise: Recht auf Vergessenwerden, Recht auf Datenübertragung oder Recht auf Widerspruch;

Art. 16, 17, 18, 19, 20, 21, 22, 23 DS-GVO;

Verzeichnis von Verarbeitungstätigkeiten

□ Erhebung sämtlicher Datenprozesse;

□ Einführung und Aufrechterhaltung einer Ablaufplanung und Organisation, damit das Verarbeitungsverzeichnis aktuell bleibt;

Art. 30 DS-GVO;

Daten von Mitarbeitern

□ Erhebung sämtlicher Datenprozesse hinsichtlich der Mitarbeiter;

□ Erfolgt die Verarbeitung der Mitarbeiterdaten, wie beispielsweise Fotos auf Firmenwebsites rechtmäßig;

□ Beachte nationale Regelungen, die aufgrund der Öffnungsklausel weiterhin anwendbar sind;

Art. 88 DS-GVO;

Technische und organisatorische Maßnahmen (TOM's)

□ Stelle sicher, dass technische und organisatorische Maßnahmen bei allen neuen Projekten umgesetzt werden, damit den Grundsätzen der Datenminimierung, der Beschränkung der Verarbeitung auf den Zweck und der Datensicherheit Genüge getan wird;

□ Umsetzung technisch-organisatorischer Maßnahmen bei bestehenden betrieblichen Abläufen;

□ Umsetzung ausreichender Maßnahmen zur Datensicherung (Sicherungskopien) und Datenvernichtung (Shreddern);

□ Einführung einer Datenschutzfolgeabschätzung;

Art. 25, 35, 36 DS-GVO;

Verträge

□ Datenschutz-Wording und Paragraphen in das Vertragswesen integrieren;

□ Überprüfung sämtlicher Verträge, die ein Datenschutz-Update benötigen;

□ Sicherstellen, dass auch Beschaffungsprozesse die Kontrolle über die Datensicherheit, Datenminimierung und Sichtbarkeit von Datenabläufen haben;

Datenschutzverletzung

□ Entwicklung einer Datenschutzverletzung-Compliance;

□ Prüfung der Versicherungspolizze für Datenschutzverletzungen;

□ Prüfung von Haftungsbestimmungen für Datenschutzverletzungen bei Dritten/Auftraggebern;

Art. 32-34 DS-GVO;

Datenexport

□ Identifiziere alle grenzüberschreitenden Datenverarbeitungen;

□ Prüfung und Anpassung der Mechanismen bei grenzüberschreitenden Datenverkehr;

□ Verwendung von Standard-Vertragsklauseln im Geschäftsverkehr mit Drittstaaten;

Art. 44-50 DS-GVO;

Ad C Laufender Betrieb

Laufende Maßnahmen

□ Laufende Fortbildung der Mitarbeiter;

□ Prüfung, ob Änderungen der Infrastruktur erfolgten;

□ Führen und Pflegen des Verfahrensverzeichnisses;

□ Anpassung der Dokumentation an die laufenden Maßnahmen;

□ Einbindung eines Datenschutzverantwortlichen/DPO bei laufenden Projekten;

□ laufende Prüfung, ob Änderung am Geschäftsmodell erfolgte oder zu den Kundenbeziehungen;

□ Prüfung, ob Änderungen der Infrastruktur oder Software erfolgten;

□ Rechtliches Update (Fortbildung der Judikatur, Änderung der Gesetzeslage, Empfehlungen der Art. 29 Gruppe, …);

Mehr Informationen finden Sie hier:

Rechtsanwaltspartnerschaft BLÜMKE & SCHÖPPL
Fadingerstraße 24/1, 4020 Linz;

Rechtsanwalt: **Mag. Peter Schöppl,**
via email: office@bluemke-schoeppl.com;
Telefon: 0732/99 70 63;