

Wichtige Punkte bei der Datenschutzverordnung (DSVGO)

Die nachfolgenden Punkte sollten Unternehmer beim Thema Datenschutz berücksichtigen. Die Mitgliedsunternehmen NUCIDA GmbH, RA Schäfer & Coll. sowie WEB9 helfen Unternehmen bei der konkreten Umsetzung der wichtigen Verordnung auf der organisatorischen, rechtlichen und technischen Ebene.



Ab 25. Mai 2018 tritt das neue Gesetz u. a. für Unternehmen verbindlich in Kraft.

Ende Mai endet für die Unternehmen die Frist, um die Vorgaben der DSGVO umzusetzen.

Sie regelt künftig den Datenschutz in der Europäischen Union. Bei Nichtbeachtung oder Verstößen sieht die neue Rechtslage einen drastisch erhöhten Bußgeldrahmen von bis zu 20 Millionen Euro vor.

- 1. Verantwortung im Unternehmen**
Datenschutz ist Chefsache, notwendig sind Datenschutzleitlinien, Beschreibung der Datenschutz-Ziele, Regelungen zu Verantwortlichkeiten und Risiken, Bestellung eines betrieblichen Datenschutzbeauftragten (wenn Voraussetzungen vorliegen, muss der Aufsichtsbehörde gemeldet werden).
- 2. Verzeichnis von Verarbeitungstätigkeiten, Artikel 30 DSGVO**
Erstellung des Verzeichnisses der Verarbeitung von personenbezogenen Daten, Berücksichtigung Privacy-by-design, Privacy-by-default (Artikel 25 DSGVO)
- 3. Prüfung der Verträge**
Überarbeitung Verträge mit Externen (Auftragsverarbeiter) (Artikel 26 - 28 DSGVO); Übersicht über Auftragsverarbeiter; besondere Anforderungen bei Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist (Garantien/ Vereinbarungen).

- 4. Betroffenenrechte und Informationspflichten**
Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren, Sicherstellung der Information der Betroffenen über alle in Artikel 13 und 14 DSGVO genannten Punkte, (auch im Internet) Sicherstellung der weiteren Betroffenenrechte (Auskunft, Berichtigung, fristgemäße Löschung der verarbeiteten Daten, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit (Artikel 15 bis 22 DSGVO).
- 5. Personenbezogene Daten von Kindern**
Sicherstellung der besonderen Anforderungen an die Einwilligung (Artikel 8 DSGVO)
- 6. Zulässigkeit der Verarbeitung**
Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, entweder einer gesetzlichen Regelung oder einer Einwilligung. Dies muss für jede Verarbeitung geprüft und dokumentiert werden. **Muster für Einwilligungserklärungen** müssen den Anforderungen von Artikel 7 und 13 DSGVO entsprechen (erweiterte Informationspflichten auch zu jederzeitigen Widerrufbarkeit der Einwilligung).
- 7. Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellung**
Dienstleister müssen technische und organisatorische Maßnahmen einsetzen, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Artikel 32 DSGVO). Dies muss dokumentiert werden, Pseudonymi-

sierung- und Verschlüsselungsverfahren sind einzusetzen, Erfordernis eines dokumentierten Rollen- und Berechtigungskonzepts, bei Änderung oder Neuentwicklung von Produkten müssen Datenschutzanforderungen von Anfang an berücksichtigt werden, regelmäßige Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen.

- 8. Datenschutzfolgenabschätzung**
Bei Verarbeitung mit einem voraussichtlichen hohen Risiko für die Rechte und Freiheiten der betroffenen Personen (Artikel 35 DSGVO) muss ein Instrument zur Beurteilung und Behandlung von Datenschutzrisiken angewendet werden (Prozess), gegebenenfalls Konsultationspflicht (Artikel 36 DSGVO).
- 9. Meldepflicht gemäß Artikel 33 DSGVO**
Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörden (Artikel 33 DSGVO). Meldefrist: 72 Stunden. Einführung einer geeigneten Methode zur Ermittlung des Risikos.
- 10. Dokumentation**
Alle in der DSGVO genannten Pflichten und Anforderungen müssen schriftlich nachgewiesen werden können. Diese Dokumentation muss immer auf dem neuesten Stand sein.