EU-Datenschutzgrundverordnung (EU-DSGVO)

Die neuen und strengeren EU-Datenschutzregeln treten am 25. Mai 2018 europaweit in Kraft mit dem Ziel, ein einheitliches Datenschutzniveau in allen EU-Mitgliedsstaaten zu erreichen.

Datenschutz wird europaweit ab Mai 2018 durch die EU-Datenschutzgrundverordnung (EU-DSGVO) neu geregelt. Dies wirkt sich auf alle Unternehmen aus, die Waren oder Dienstleistungen für EU-Bürger anbieten und Daten von Kunden in der EU speichern. Unternehmen müssen ihre Prozesse im Umgang mit personenbezogenen Daten an die strengeren Anforderungen der EU-DSGVO anpassen.

Point of View Branche:

Gespeicherte Daten und Data Mining (Big data) sind wertvoll und viele Unternehmen verwenden diese Daten, um auch Werbung gezielt zu verbreiten. Als Maßnahme u.a. gegen möglichen Datenmissbrauch wurde die EU-DSGVO im Mai 2016 im EU-Amtsblatt veröffentlicht. Nach einer Übergangsfrist wird diese Verordnung zum 25. Mai 2018 in allen EU-Staaten geltendes Recht und größtenteils das bisherige Bundesdatenschutzgesetz ersetzen.

Adressaten der EU-DSGVO sind alle Unternehmen jeder Größenordnung und jeder Branche mit Sitz oder Niederlassung in der EU, die personenbezogene Daten verarbeiten. Dies gilt auch für Unternehmen, wenn sie außerhalb der EU ihren Firmensitz haben, jedoch Daten von EU-Bürgern verarbeiten.

Was soll die EU-DSGVO bewirken?

- Softwareentwicklung: Datenschutz durch Technik und datenschutzfreundliche Voreinstellung („privacy by design and by default“)
- Datenübertragbarkeit: Kompatibilität durch geeignetes Datenformat, hohe Anforderungen an die Übermittlung an Drittstaaten
- Recht auf „Vergessenwerden“: Auf Anfrage steht EU-Bürgern zu, dass ihre veralteten Daten gelöscht oder korrigiert werden
- Transparenz: Die Verarbeitungslinie der Daten muss aufzeigen, wo sich personenbezogene Daten befinden und wie diese genutzt bzw. verarbeitet werden
- Marktortprinzip: Nicht der Ort, wo sich die Daten von EU-Bürgern befinden ist entscheidend, sondern die Tatsache, dass es sich um Daten von EU-Bürgern handelt
- Auslagerung und gemeinsame Haftung: Werden externe Dienstleister mit der Datenverarbeitung beauftragt, haften beide Unternehmen für einen Verstoß
- Datenschutzverstöße: Meldung innerhalb von 72 Stunden an Datenschutzbehörde und Betroffenen
- Nachweis: Das Unternehmen muss bei Verdacht auf einen Verstoß nachweisen, dass der Datenschutz rechtmäßig eingehalten wurde
- Hohe Strafen: Bis zu 4% des gesamten weltweit erzielten Jahresumsatzes einer Unternehmensgruppe, maximal EUR 20 Mio.

Nationale Ergänzungsregelungen:

Am 27.04.2017 verabschiedete der Deutsche Bundestag den „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die EU-Verordnung 2016/679 und zur Umsetzung der EU-Richtlinie 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz, DSAnpUG-EU). Das neue Datenschutzgesetz wird die EU-DSGVO ergänzen. Der Grund dafür ist, dass die EU-DSGVO den Mitgliedsstaaten über sog. Öffnungsklauseln zahlreiche Möglichkeiten

einräumt, in bestimmten Bereichen eigene datenschutzrechtliche Regelungen aufzustellen.

Welche Unternehmen müssen einen Datenschutzbeauftragten (DSB) benennen?

Einen DSB benötigen gemäß Artikel 37 der DSGVO alle Unternehmen, in denen personenbezogene Daten automatisiert verarbeitet werden. Die Verarbeitung umfasst die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten mittels PC. Ergänzend regelt das BDSG § 38 die Voraussetzungen für die Ernennung eines Datenschutzbeauftragten. Die Ernennung eines DSB wird für Unternehmen mit mehr als neun Mitarbeitern Pflicht, sofern es diesen - auch nur theoretisch - möglich ist, ständig personenbezogene Daten automatisiert zu verarbeiten.

Welches sind die drei Pfeiler der Datenschutzdokumentation?

1. Dokumentation der Notwendigkeit einer Datenschutz-Folgenabschätzung (DSFA): Die Unternehmen sind angehalten, Ihre Verarbeitungsprozesse hinsichtlich personenbezogener Daten auf Datenschutzrisiken hin zu analysieren, zu dokumentieren und ständig zu überprüfen. Nach einer Risikoanalyse durch das Unternehmen ist zu entscheiden, ob eine DSFA gemäß Art. 35 EU-DSGVO durchzuführen ist, oder nicht. Diese Entscheidung ist auf jeden Fall schriftlich für jeden konkreten Verarbeitungsvorgang zu begründen. Die Datenschutzrisiken sind nach „objektiven Kriterien“ aus Sicht des eventuell Betroffenen zu ermitteln (Erwägungsgrund 76 und Art. 71 BDSG (neu) Abs. 1).

2. Erstellung eines Verfahrensverzeichnisses sowie Erfassung der Auftragsdatenverarbeiter:

Ein internes Verzeichnis von Verarbeitungs-tätigkeiten (Verfahrensverzeichnis) nach EU-DSGVO müssen sowohl Verantwortliche für den Datenschutz, als auch Auftragsverarbeiter (Auftragsdatenverarbeiter), führen. Dabei muß der Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung erstellen.

3. Dokumentation der Sicherheit der Verarbeitung, also der technischen und organisatorischen Maßnahmen (TOM):

Die Dokumentation der TOM als 3. Pfeiler ist ebenso eine zentrale und verpflichtende Datenschutzdokumentation. Die TOMs „überwachen“ den gesamten Datenschutz im Unternehmen: Wie werden die Daten der Betroffenen (Kunden, Lieferanten, Mitarbeiter etc.) geschützt und gesichert.

Point of View Kunde:

Die neuen Datenschutzregeln haben Einfluss auf die gesamte Unternehmensorganisation, ihre Governance und die internen Prozesse. Folgende Themen müssen Unternehmen besonders beachten:

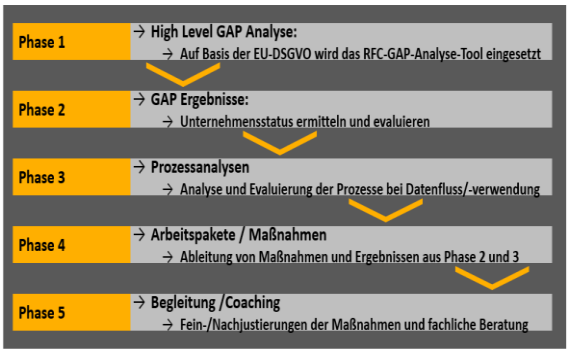
- Verantwortung, Zuständigkeiten
- Unternehmensorganisation, Nachweispflicht
- Betroffenheit und Rechte der Dateninhaber
- Interne Prozesse, Sicherheitskonzepte
- Datenverarbeitungssituationen im Unternehmensumfeld
- Besonderheit bei der externen Auslagerung der Datenverarbeitung

Die Unternehmen haben den Rahmen für die Handlungsfelder anzupassen und interne Kontrollsysteme zur Sicherstellung aufzubauen, um den Regeln zur Verschärfung des Datenschutzes zu entsprechen. Dabei sind in aller Regel Prozessanpassungen in Bezug auf das Datenschutzmanagementsystem zu berücksichtigen.

Point of View Lösung:

Die durch die EU-DSGVO gestellten Anforderungen erhöhen den Aufwand für Compliance- und IT-Ressourcen, nicht zuletzt aufgrund der Bewertung und Abwägung der Risiken der Datenrechte vor der eigentlichen Verarbeitung. Für alle Neuerungen in der

DSGVO bietet sich ein mehrstufiges Vorgehen an, für das wir folgenden Handlungsfahrplan ausgearbeitet haben:



Phase 1) High Level Gap Analyse: Mit Hilfe des RFC GAP-Analyse-Tools werden die Ergebnisse eines detaillierten Fragebogens ausgewertet, der Fragen aus 21 Handlungsfeldern auf Basis der DSGVO enthält.

Phase 2) GAP Ergebnisse: Die Ergebnisse der GAP-Analyse werden auf ihre Auswirkungen und ihren Umsetzungsbedarf mit Dringlichkeiten je Geschäftsbereich hin analysiert, um die Bedarfe festzulegen und ein Datenschutzkonzept inkl. Handlungsfeldern und Schwerpunktbereichen mit Prioritäten zu erstellen.

Phase 3) Prozessanalysen: Die Auswirkungen der Ergebnisse auf die internen Prozesse je Geschäftsbereich werden umfassend evaluiert und auf Konformität zur DSGVO überprüft, u.a. hinsichtlich Datenfluss und -verwendung.

Phase 4) Arbeitspakete/Maßnahmen: In einem weiteren Schritt werden die Ergebnisse aus Phase 2 und 3 aus der Toolanwendung und den Prozessanalysen umfassend evaluiert, um daraus Arbeitspakete festzulegen und entsprechende Handlungsmaßnahmen und -empfehlungen abzuleiten. Dies beinhaltet auch die Erstellung von Templates, Richtlinien, Verfahrensverzeichnissen, technischen und organisatorischen Maßnahmen (TOM), sowie Datenschutzfolgenabschätzungen (DSFA).

Phase 5) Begleitung/Coaching: Abschließend ist die Begleitung und fachliche Beratung der Implementierung inkl. Erstellung von Statusberichten zur Compliance- und Risikosituation sicherzustellen, damit die Verantwortlichen interne Prozesse effektiv steuern und überprüfen können.

Point of View Mehrwert:

Die folgenden Mehrwerte bietet der RFC-Ansatz auf dem Weg hin zu einer erfolgreichen Implementierung der EU-DSGVO:

- Hohe Qualitätsstandards unserer zertifizierten Projekt- und Testmanager
- Soll/Ist Vergleich des bestehenden Geschäftsmodells auf Basis der regulatorischen Anforderungen, mit Hilfe des RFC-DSGVO-Tools
- Ableitung eines Maßnahmenkatalogs mit Schwerpunktbereichen und Prioritäten
- Evaluierung des finalen Diagnoseergebnisses inkl. Begleitung und fachlicher Beratung hinsichtlich Implementierung und Steuerung

RFC Professionals hat ein stringentes Beratungskonzept für die Umsetzung der neuen EU-DSGVO und wird Ihr Unternehmen hierbei nachhaltig unterstützen.

Ihre Ansprechpartner:

Oliver Tiebing Senior Partner	Mobil: +49 171 569 4276 Mail: oliver.tiebing@RFC-Professionals.com
Peter Sperl Head of Industry	Mobil: +49 151 422 40792 Mail: peter.sperl@RFC-Professionals.com
Henrik Hansen Manager	Mobil: +49 151 422 40 776 Mail: henrik.hansen@RFC-Professionals.com