Newsletter Recht aktuell Issue 1|2017 – Datenschutz-Grundverordnung Teil 2

Auswirkungen der DSGVO auf Organisation und Prozesse

1. Einleitung

Die Datenschutz-Grundverordnung („DSGVO") bringt umfangreiche neue Anforderungen für Unternehmen. Die folgende Darstellung gibt einen Überblick über die Auswirkungen der DSGVO auf die Organisation und Prozesse in einem Unternehmen und bietet Lösungsansätze. Ab 25.05.2018 trifft jedes Unternehmen zahlreiche Pflichten.

2. Neue Verpflichtungen für Unternehmer

- Erweiterte Dokumentations- und Nachweispflichten

  Die DSGVO sieht deutlich erweiterte Dokumentations- und Nachweispflichten sowohl für verantwortliche Unternehmen als auch Auftragsverarbeiter (Dienstleister) vor. Das verantwortliche Unternehmen muss nachweisen können, dass es die in Art 5 DSGVO normierten Datenschutzgrundsätze einhält und die Daten in Übereinstimmung mit der DSGVO verarbeitet. Der Art 5 DSGVO nominiert folgende: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht.

  Auftragsverarbeiter müssen dem verantwortlichen Unternehmen alle erforderlichen Informationen zur Verfügung stellen, damit dieses nachweisen kann, seine datenschutzrechtlichen Pflichten erfüllt zu haben.

  Verstößt ein verantwortliches Unternehmen gegen diese Anforderungen, drohen Bußgelder von bis zu 4 % des Umsatzes.

  Wir empfehlen daher, umgehend mit der Etablierung eines entsprechenden Datenschutz-Management-Systems nach dem Vorbild entsprechender Compliance-Strukturen zu beginnen.

- Transparenz und Informationspflichten

  Künftig müssen Unternehmer betroffene Personen deutlich umfassender als bislang und in nachvollziehbarer Weise darüber informieren, ob und wie sie Daten verarbeiten. Das Unternehmen muss betroffene Personen von der Verarbeitung ihrer personenbezogenen

Daten *„in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache*" unterrichten. Die Art 12 bis 15 DSGVO sehen dabei umfangreiche Auskunftsrechte betroffener Personen und Auskunftspflichten verantwortlicher Unternehmen vor, die deutlich über die bisherigen Vorgaben hinausgehen.

Verstöße gegen diese Pflichten können zu hohen Bußgeldstrafen von bis zu 4 % des Umsatzes führen.

Wir empfehlen daher, die erforderlichen Schritte vorzunehmen, um diese Anforderungen überhaupt erfüllen zu können (zB zeitnahe Anfertigung und Zurverfügungstellung von Kopien an die betroffene Person, Anpassung der bestehenden IT-Strukturen usw).

- Verzeichnis der Verarbeitungstätigkeiten

Art 30 DSGVO schreibt vor, dass das verantwortliche Unternehmen ein umfassendes Verzeichnis aller Verarbeitungstätigkeiten zu führen hat. Dieses Verarbeitungsverzeichnis ist eines der zentralen Instrumente zur Umsetzung der Dokumentationspflichten nach Art 24 DSGVO. Das Verarbeitungsverzeichnis ist schriftlich oder in elektronischer Form zu führen und hat sämtliche Datenverarbeitungsvorgänge zu enthalten.

Ausnahmen von der Verpflichtung, ein Verarbeitungsverzeichnis zu führen, gibt es unter bestimmten Voraussetzungen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Aufgrund der bestehenden Dokumentationspflicht empfehlen wir jedoch jedenfalls ein Verarbeitungsverzeichnis zu führen.

Fehler bei der Erstellung des Verarbeitungsverzeichnisses werden mit Geldbußen von bis zu 2 % des Umsatzes geahndet.

Unternehmen sollten daher prüfen, ob und in welchem Umfang sie Informationen im Verarbeitungsverzeichnis dokumentieren müssen, um ihren Pflichten nach Art 24 DSGVO nachzukommen. Eine möglichst effektive Dokumentation datenschutzrelevanter Vorgänge kann das Risiko von Bußgeldern und anderer Nachteile erheblich verringern.

- Datenschutzfolgeabschätzung

Hat eine Datenverarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der davon betroffenen Personen zur Folge, so muss das verantwortliche Unternehmen eine Datenschutzfolgenabschätzung nach Art 35 DSGVO durchführen.

Hierbei soll das verantwortliche Unternehmen insbesondere die Eintrittswahrscheinlichkeit und Schwere des möglichen Risikos bewerten. Das Unternehmen soll dabei Art, Umfang, Umstände, verfolgte Zwecke sowie Ursachen möglicher Risiken für Rechte und Freiheiten betroffener Personen bewerten. Dabei soll es auch Maßnahmen, Garantien und Verfahren prüfen, mit denen Unternehmen bestehende Risiken eindämmen und die sonstigen Vorgaben der DSGVO einhalten können.

Sofern die Datenschutzfolgenabschätzung ergibt, dass die geplante Datenverarbeitung tatsächlich ein hohes Risiko zur Folge hätte, muss das Unternehmen die Datenschutzbehörde zu Rate ziehen, sofern es keine Maßnahmen zur Eindämmung des Risikos trifft.

Unterlässt das Unternehmen eine vorgeschriebene Datenschutzfolgenabschätzung oder führt diese nicht korrekt durch, drohen Geldbußen von bis zu 4 % des Umsatzes.

Die Datenschutzfolgenabschätzung ersetzt die bisherige Meldepflicht an die Datenschutzbehörde und ist daher ein wichtiges Mittel, um die Dokumentationspflichten von Unternehmen zu erfüllen und Risiken in Bezug auf den Datenschutz effektiv bewerten zu können. Auch aus diesem Grund sollten Unternehmen zeitnah Strukturen und Prozesse schaffen, um die detaillierten Anforderungen an die Datenschutzfolgenabschätzung spätestens bis zum Inkrafttreten der DSGVO zu erfüllen.

- Privacy by Design (Datenschutz durch Technik)

  Unternehmen müssen gemäß Art 25 Abs. 1 DSGVO ihre IT-Systeme so ausgestalten, dass sie die Datenschutzgrundsätze des Art 5 DSGVO wirksam umsetzen.

- Privacy by Default

  Unternehmen müssen ihre IT-Systeme gemäß Art 25 Abs 2 DSGVO so voreinstellen, dass sie grundsätzlich nur solche personenbezogenen Daten verarbeiten, deren Verarbeitung für den jeweils verfolgten Zweck erforderlich ist.

- Datensicherheit

  Es besteht aufgrund der DSGVO eine erweiterte Verpflichtung zur Implementierung technischer und organisatorischer Schutzmaßnahmen, um die Datensicherheit zu gewährleisten. Diese sollen ein dem jeweiligen Risiko angemessenes Schutzniveau gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten sowie

Zwecke, Art, Umfang und Umstände der Verarbeitung zu berücksichtigen. Einzelne Maßnahmen können zB Pseudonymisierung und Verschlüsselung von Daten, Recovery usw sein.

3. Fazit

Die Pflichten und Anforderungen an Unternehmen werden durch die neue Datenschutz-Grundverordnung erheblich ausgeweitet. Die DSGVO betrifft jeden Unternehmer, der nur irgendeiner Art und Weise personenbezogene Daten erfasst oder verarbeitet.

Aufgrund der Vielzahl an Änderungen, insbesondere der zukünftigen unternehmensinternen Verantwortlichkeiten und dem teils großen technischen und organisatorischen Handlungsbedarf, empfehlen wir Unternehmen unbedingt, umgehend mit der Umsetzung der DSGVO zu beginnen.

Information

Mag. Monika Sturm
T +43 1 535 8008, Em.sturm@mplaw.at

Mag. Claudia Fleischhacker-Hofko
T + 43 1 535 8008, E c.fleischhacker@mplaw.at

Müller Partner Rechtsanwälte GmbH
Rockhgasse 6, 1010 Wien
www.mplaw.at