Neue EU-Datenschutz-Grundverordnung (DSGVO)

Gut gewappnet für die umfänglichen Reformen im europäischen Datenschutz

Das Inkrafttreten der DSGVO bedeutet für Unternehmen aller Branchen umfangreiche neue Anforderungen und veränderte Fristen bei zugleich drastisch erhöhten Sanktionen. Es besteht akuter Handlungsbedarf: Bereits am 25. Mai 2018 wird die DSGVO zu unmittelbar geltendem Recht. KPMG unterstützt bei der zeitnahen Umsetzung der umfänglichen Vorgaben.

Die Herausforderung

Die DSGVO bringt ein völlig neues Datenschutzregime mit sich. Sie zielt auf die Einrichtung eines Datenschutzmanagementsystems ab. Die bisherigen Zuständigkeiten, Prozesse und Maßnahmen müssen neu bewertet werden. Risikoanalyse, Konzeption und Transparenz rücken in den Vordergrund. Das Verzeichnis der Verarbeitungstätigkeiten wird zum zentralen Dokumentations- und Steuerungselement.

Die DSGVO sieht vor allem folgende Neuerungen vor:

- massiv erweiterte Sanktionen (bis 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Vorjahresumsatzes)
- erweiterte Haftungsrisiken (Rechenschaftspflicht)
- neue Fristen und Transparenzpflichten
- verschärfte Notifikationspflichten bei Datenschutzverstößen (72-Stunden-Frist)
- Erfordernis einer auf einer Risikoanalyse basierenden Datenschutz-Folgenabschätzung
- „Privacy by Design“ und „Privacy by Default“
- neue Anforderungen an das Verfahrensverzeichnis
- erweiterte Informations- und Hinweispflichten
- erweiterte Betroffenenrechte (insbesondere Recht auf Datenportabilität und Recht auf Vergessenwerden)
- neue Anforderungen an die Einwilligung
- neue Anforderungen an die Auftragsverarbeitung

Zudem räumen Öffnungsklauseln den nationalen Gesetzgebern in einzelnen Bereichen Gestaltungskompetenzen ein. Der deutsche Gesetzgeber hat diese zum Teil bereits im neuen Bundesdatenschutzgesetz (BDSG) umgesetzt. Allerdings stehen Änderungen an spezialgesetzlichen Datenschutzregelungen nach wie vor aus. Wichtig: Auch außerhalb der EU ansässige Unternehmen haben die DSGVO zu beachten, sofern sie Daten von in der EU befindlichen Personen zum Angebot von Waren und Dienstleistungen oder zur Verhaltensbeobachtung verarbeiten.

In Anbetracht der Vielfältigkeit der zu implementierenden Prozesse und Maßnahmen ergibt sich in der verbleibenden Zeit ein erhöhter Aufwand, den Anforderungen der DSGVO in organisatorischer, prozessualer und technischer Hinsicht gerecht zu werden. Wer besonders viele oder besonders schützenswerte Daten verarbeitet oder in besonderem Maße neue Technologien einsetzt, wird einen größeren Aufwand betreiben müssen als andere Unternehmen.

In Bezug auf die DSGVO-Vorgaben sollten Unternehmen insbesondere Folgendes prüfen:

- ✓ Verfügt das Unternehmen über ein ganzheitliches Datenschutzkonzept im Sinne eines Managementsystems?
- ✓ Verfügt das Unternehmen über ein vollständiges Verzeichnis aller Verarbeitungstätigkeiten?
- ✓ Ist zweifelsfrei geklärt, wann eine Datenschutz-Folgenabschätzung inklusive Konsultation der Aufsichtsbehörde durchzuführen ist?
- ✓ Sind Zuständigkeiten und Prozesse implementiert, die sicherstellen, dass Informations- und Transparenzpflichten erfüllt und Fristen eingehalten werden?
- ✓ Ist Ihr Unternehmen im Falle eines Datenschutzverstoßes umfassend reaktionsfähig und kann die 72-Stunden-Meldepflicht einhalten?
- ✓ Werden die Grundsätze „Privacy by Design" und „Privacy by Default" bei der Implementierung technischer und organisatorischer Maßnahmen berücksichtigt?
- ✓ Wurden geeignete Prozesse und Maßnahmen eingerichtet, um Datenportabilität zu gewährleisten?
- ✓ Verfügt das Unternehmen über ein geeignetes Löschkonzept dafür, Löschbegehren nachzukommen, insbesondere auch in Bezug auf Prozesse zur Information Dritter, denen die Daten offengelegt wurden?
- ✓ Genügen die bisherigen Prozesse zur Einholung einer Einwilligung des Betroffenen auch den gestiegenen Anforderungen der DSGVO?
- ✓ Wie werden internationale Datentransfers gehandhabt? Welche Maßnahmen werden genutzt – und entsprechen diese den geforderten neuen Vorgaben?
- ✓ Genügen Verträge mit Auftragsverarbeitern den Anforderungen der DSGVO?
- ✓ Werden auf Basis der Öffnungsklauseln erlassene nationale Vorschriften berücksichtigt?

Unsere Leistung

KPMG steht Ihnen bei allen Fragen rund um das Thema EU-Datenschutz-Grundverordnung und deren Implementierung mit umfangreicher Erfahrung aus zahlreichen Projekten und breitem Know-how zur Seite. Auf Basis einer Gap-Analyse unterstützen wir Sie bei der Konzeption und Implementierung eines Datenschutzmanagementsystems mit seinen Kerndatenschutzprozessen, Risikoanalysen und der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten. Auch für die Umsetzung einzelner Maßnahmen, wie die Konzeptionierung eines unternehmensweiten Löschkonzepts, die Sicherstellung der Transparenzanforderungen oder des Dienstleistermanagements im Rahmen der Auftragsverarbeitung und Drittstaatenübermittlung stehen wir zur Verfügung. Darüber hinaus führen wir Wirksamkeitsprüfungen des Datenschutzmanagementsystems nach anerkannten Standards durch.

Daneben helfen Ihnen unsere interdisziplinären Experten auch im Ernstfall. Im Falle von Verstößen gegen Datenschutz- oder Datensicherheitsregeln unterstützen wir Sie bei der Aufklärung und Aufarbeitung und geben Empfehlungen zur Neuausrichtung der Prozesse und Systeme.

Bestens für Sie aufgestellt

Der Bereich Compliance & Forensic von KPMG arbeitet eng mit Branchen- und IT-Experten zusammen, verfügt über umfassende Erfahrung und Praxisorientierung auf dem Gebiet der Datenschutzberatung und ist mit allen regulatorischen Anforderungen und Standards vertraut. Unsere Spezialisten stehen Ihnen deutschlandweit zur Verfügung. Zudem können wir aufgrund unserer Einbindung in das weltweite KPMG-Netzwerk auf das Know-how weiterer Experten zurückgreifen, die bei internationalen Fragestellungen und Sachverhalten kompetent unterstützen. So profitieren Sie von unserem profunden Verständnis für Märkte, Branchen und Unternehmen.

Gerne stehen wir für Ihre Fragen oder ein erstes Gespräch zur Verfügung. Sprechen Sie uns an.

Kontakt

KPMG AG Wirtschaftsprüfungsgesellschaft

Barbara Scheben
Partner, Compliance & Forensic
T +49 69 9587-3737
bscheben@kpmg.com

Niels Litzka
Senior Manager, Compliance & Forensic
T +49 69 9587-1417
nlitzka@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia