FREY RECHTSANWÄLTE
RECHTSMANAGEMENT · STRATEGISCHE BERATUNG

Status Quo

Ausgabe II - Februar 2018

Compliance: Der Countdown läuft – noch wenige Wochen, dann gilt die Datenschutz-Grundverordnung

Kaum ein Thema wird unter Compliance-Gesichtspunkten aktuell mehr diskutiert, als die Umsetzung der europäischen Datenschutz-Grundverordnung (DS-GVO): Warum ist das so? Wie lässt sich die verbleibende Zeit sinnvoll für eine Risikominimierung nutzen?

I. Stichtag: 25. Mai 2018

Ab dem 25. Mai 2018 gilt die DS-GVO, die dann unmittelbar in allen EU-Mitgliedstaaten Anwendung findet. Eines weiteren Rechtsaktes, wie z. B. bei der Umsetzung von Richtlinien, bedarf es für die Geltung der Verordnung nicht.

Nicht alle Unternehmen haben sich bisher im Rahmen ihrer Geschäftsabläufe mit den neuen Vorgaben der DS-GVO und dem damit einhergehenden Anpassungsbedarf von Prozessen ausreichend befasst. Der Countdown läuft…

II. Risiko: Geldbußen bis zu 20 Mio. EUR und Schadensersatz

Grund für die hohe Sensibilität im Hinblick auf die DS-GVO ist ein Paradigmenwechsel des Gesetzgebers bezüglich der Höhe möglicher Geldbußen. Bei Verstößen sind ab dem 25. Mai 2018 nicht mehr nur – wie bislang im Bundesdatenschutzgesetz (BDSG) vorgesehen – Geldbußen bis zu 300.000 EUR möglich, sondern bis zu 20. Mio. EUR bzw. bei Unternehmen sogar von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

Außerdem sieht die DS-GVO bei Verstößen einen Anspruch auf Schadensersatz wegen materieller und immaterieller Schäden vor. Eine Haftungsbefreiung kommt nur in Betracht, wenn das Unternehmen den Nachweis erbringt, dass es in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Das Unternehmen trägt also die volle Beweislast für die Einhaltung der DS-GVO.

Mit einem u. U. existenzgefährdenden Sanktionsrahmen verfügt die DS-GVO über ein sehr scharfes Schwert. Die Beachtung der Regelungen der DS-GVO im Unternehmen ist unter Compliance-Gesichtspunkten daher zwingend erforderlich.

III. Risiko: Unternehmensführung ist verantwortlich

Verantwortlich für die ordnungsgemäße Umsetzung der DSG-VO ist der Vorstand beziehungsweise die Geschäftsführung eines Unternehmens.

Bei Verstößen können die Aufsichtsbehörden nicht nur hohe Geldbußen gegen das Unternehmen verhängen. Die Verantwortlichen haften u. U. auch persönlich, d. h. mit ihrem Privatvermögen. Zwar sichern D&O-Versicherungen Vorstände und Geschäftsführer regelmäßig gegen Risiken ab, bei grober Fahrlässigkeit wird die Versicherung aber oftmals nicht für den Schaden eintreten. Grobe Fahrlässigkeit kann bereits dann vorliegen, wenn dem Verantwortlichen nachgewiesen werden kann, dass er bei Verstößen gegen das Datenschutzrecht untätig geblieben ist.

Die Unternehmensführung ist folglich – auch in Anbetracht einer möglichen persönlichen Inanspruchnahme – angehalten, die

Umsetzung der Vorgaben der DS-GVO im Unternehmen sicher zu stellen.

VI. Risiko: Gefährdung des Unternehmenswerts

Sofern personenbezogene Daten im Unternehmen nicht rechtmäßig verarbeitet werden, gefährdet der hohe Sanktionsrahmen der DS-GVO den Unternehmenswert in zweifacher Hinsicht: Zum einen setzt sich das Unternehmen der Gefahr hoher Geldbußen aus, zum anderen sind personenbezogene (Kunden-)Daten, die ein Unternehmen unter Missachtung der DS-GVO aggregiert (hat), wertlos: rechtswidrig erhobene personenbezogene Daten dürfen nicht mehr genutzt werden.

Dies gilt vor allem dann, wenn das Geschäftsmodell des betreffenden Unternehmens maßgeblich auf personenbezogenen Daten aufbaut oder diese gar dessen USP ausmachen. Im Zuge der stetig steigenden Bedeutung von Big-Data-Anwendungen in nahezu allen Branchen und der rasant fortschreitenden digitalen Transformation trifft dies auf immer mehr Unternehmen zu.

Daraus folgt auch, dass Unternehmenskäufe und -verkäufe nicht mehr ohne eine belastbare Datenschutz-Due Diligence auskommen werden, will ein Erwerber keine risikobehaftete und u.U. wertlose Black-Box akquirieren.

Die Einhaltung der Datenschutz-Compliance ist damit nicht nur wegen der unmittelbar drohenden Geldbußen, sondern auch für die Sicherung nachhaltiger und realisierbarer Unternehmenswerte auf der Grundlage rechtmäßig aggregierter und verwendbarer personenbezogener Daten relevant.

V. Risikominimierung

Die Zeit drängt. Ist eine vollständige Anpassung von Unternehmensprozessen an die DS-GVO in der verbleibenden Zeit nicht mehr möglich, rückt die Frage, wie sich bestehende Risiken minimieren lassen, in den Mittelpunkt.

Bei der Entscheidung über die Verhängung einer Geldbuße muss eine Aufsichtsbehörde einen umfassenden Katalog verschiedener Kriterien berücksichtigen, u. a. Art, Schwere und Dauer des Verstoßes und zwar unter Beachtung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung wie auch die Anzahl der von der Verarbeitung betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens. Das bedeutet auch: Unternehmen, die sich bislang noch nicht mit den Vorgaben der DS-GVO auseinandergesetzt haben, können auch zum jetzigen Zeitpunkt in einem ersten Schritt Risiken minimieren:

Wie geht man besten vor? Ausgangspunkt ist immer eine Bestandsaufnahme des *status quo*, bei der das rechtlich erforderliche Verzeichnis über alle Verarbeitungstätigkeiten personenbezogener Daten erstellt wird. Es ist festzustellen, ob die vorhandenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten auch nach neuer Rechtslage ausreichen. Aufbauend auf der Bestandaufnahme lassen sich dann die verschiedenen Verarbeitungsprozesse personenbezogener Daten sowie die erforderlichen Dokumente, wie z. B. Einwilligungen oder Datenschutzhinweise, erstellen bzw. anpassen. So müssen beispielsweise die Datenschutzhinweise nach der neuen Rechtslage alle für die Verwendung personenbezogener Daten einschlägigen Rechtsgrundlagen enthalten. Der Kunde ist explizit über seine Rechte aufzuklären.

Zusätzlich ist bei geplanten Verarbeitungsprozessen, die ein hohes Risiko für die Rechte und Freiheiten betroffener Personen bergen, eine sogenannte Datenschutz-Folgenabschätzung durchzuführen, um Risiken entsprechend minimieren zu können.

VI. *Exkurs*: Recht auf Datenübertragbarkeit

Die DS-GVO sieht zugunsten betroffener Personen, also derer, deren persönliche Daten verarbeitet werden, eine Reihe von Rechten vor. Hierzu gehört auch das neu geschaffene Recht auf Datenübertragbarkeit (Art. 20 DS-GVO).

Danach kann ein Kunde jederzeit die Übermittlung seiner personenbezogenen Daten, die er einem Unternehmen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format verlangen. Das Recht auf Datenübertragbarkeit reicht aber noch weiter: Der Kunde kann zusätzlich erwirken, dass seine Daten direkt an ein anderes Unternehmen – z. B. einen Wettbewerber – ohne Behinderungen übermittelt werden.

.

*Wie ist das Recht auf Datenübertragbarkeit im Einzelnen ausgestaltet? Welche Daten sind betroffen? Diese und viele andere Fragen beleuchten wir in unserem **Special zum Recht auf Datenübertragbarkeit** unter **frey.eu**. Erfahren Sie mehr über dieses neue Recht der DS-GVO.*

V.i.S.d.P./V.i.S.d. §§ 5 TMG, 55 Abs. 2 RStV: Prof. Dr. Dieter Frey
FREY Rechtsanwälte Partnerschaft | Agrippinawerft 22 (Rheinauhafen) | D-50678 Köln | Tel. +49 221 42 07 48-00 | Fax. +49 221 42 07 48-29 | info@frey.eu
Vertretungsberechtigte Partner RA Prof. Dr. Dieter Frey, LL.M. (Brügge), RA Dr. Matthias Rudolph
Partnerschaftsregister des Amtsgerichts Essen, PR 2631
Umsatzsteueridentifikationsnummer: DE 281 489 395
Zuständige Rechtsanwaltskammer: Rechtsanwaltskammer Köln | Riehler Straße 30 | 50668 Köln
Berufshaftpflichtversicherung: ERGO Versicherungsgruppe AG vormals: VICTORIA Versicherung AG | Victoriaplatz 2 | 40477 Düsseldorf
Der räumliche Geltungsbereich des Versicherungsschutzes umfasst Tätigkeiten in den Mitgliedsländern der Europäischen Union und genügt so mindestens den Anforderungen des § 51 Bundesrechtsanwaltsordnung (BRAO).