
Foto: istockphoto | welcomia

DSGVO: Neue Pflichten beim Datenschutz

Am 25. Mai tritt die neue Datenschutz-Grundverordnung DSGVO in Kraft. Damit sollen Personendaten innerhalb der EU einheitlich geschützt werden. Dass dieses Regelwerk auch Finanzdienstleister betrifft, ist vielen nicht bewusst. Dabei drohen bei Verstößen empfindliche Bußgelder

von Elton Mikulic, Rechtsanwalt bei Otto Mittag Fontane

Von anonymen Hackerangriffen über Sicherheitslücken bis hin zum politischen Missbrauch von Daten aus sozialen Netzwerken – die Grenzen und Risiken der Verarbeitung und der Analyse großer Datenmengen sind in aller Munde. Passend hierzu tritt am 25. Mai 2018 die Verordnung (EU) 2016/679 vom 27. April 2016 (Datenschutz-Grundverordnung; DSGVO) in Kraft. Ihr Zweck ist einerseits der Schutz personenbezogener Daten natürlicher Personen und andererseits die Gewährleistung eines freien und rechtssicheren Verkehrs solcher Daten innerhalb der Union sowie durch die Stärkung des Verbrauchervertrauens auch die Schaffung eines regulierten digitalen Binnenmarktes. Als europaweit unmittelbar geltendes Recht lässt die Verordnung nur wenige Gestaltungsspielräume für nationale Sondervorschriften. Trotz eines zweijährigen Übergangszeitraums scheint sich aber noch nicht bei allen Finanzdienstleistern herumgesprochen zu haben, dass dieses Regelungswerk unter anderem auch für Wertpapierunternehmen, gewerbliche Vermögensberater und Vermittler unabhängig von ihrer Größe einige wesentliche Änderungen im Datenschutzrecht mit sich bringt.

Sehr weiter Anwendungsbereich

Die Verordnung ist auf die automatisierte Verarbeitung sowie die nicht-automatisierte Verarbeitung personenbezogener Daten anwendbar, soweit sie in einem Dateisystem gespeichert werden. Der Begriff der Verarbeitung ist hierbei weit auszulegen. Er reicht von der Erfassung über die Ordnung, Speicherung, Auswertung und Bereitstellung bis zur Löschung und Vernichtung von

Elton Mikulic,
Otto Mittag Fontane, Frankfurt am Main

Daten. Von erheblicher Tragweite ist vor allem das neu eingeführte „Marktortprinzip“. Das bedeutet: Datenverarbeitende Unternehmen oder Auftragsverarbeiter mit Sitz oder Niederlassung in der EU werden automatisch von der DSGVO erfasst, gleichgültig ob die Daten innerhalb oder außerhalb der EU verarbeitet werden. Aber auch Unternehmen mit keiner physischen Organisations- oder Betriebsstruktur innerhalb der EU sind Adressaten der Verordnung. Grundsätzlich sind alle Unternehmen betroffen, die Daten im Zusammenhang mit dem Angebot von Waren und Dienstleistungen an Personen innerhalb der EU verarbeiten, unabhängig davon, ob ein Entgelt für die Waren oder Dienstleistungen gefordert wird (also auch soziale Netzwerke). Ferner ist die Verordnung aber auch in Fällen anwendbar, bei denen lediglich das Verhalten von Personen innerhalb der EU beobachtet wird (z.B. durch Tracking-Cookies). In allen diesen Fällen müssen die betroffenen Unternehmen einen in einem betroffenen EU-Mitgliedsstaat niedergelassenen Vertreter bestellen, der gegenüber Verbrauchern und Aufsichtsbehörden als Anlaufstelle dient.

Verantwortlichkeiten zuordnen

Das kann insbesondere bei Finanzdienstleitern problematisch werden. Denn nicht selten besteht hier ein Geflecht von Datenflüssen zwischen mehreren Unternehmen wie Emittenten, Vermögensverwaltern, Vermittlern, Haftungsdächern, Werbepartnern und Depotbanken. Die Zuordnung von Verantwortlichkeiten ist daher von höchster Relevanz. Gemäß der neuen Verordnung gilt das Unternehmen als Verantwortlicher der Datenverarbeitung, das über die Zwecke und die Mittel der Datenverarbeitung entscheidet. Dieses darf die Verarbeitung zwar sogenannten Auftragsverarbeitern überlassen, auf die künftig mehr Verantwortung und mehr Pflichten zukommen. Dem muss aber stets eine Prüfung der Geeignetheit

des Auftragsverarbeiters durch den Verantwortlichen vorangehen. In der Praxis wird diese Prüfung anhand vorgewiesener Zertifizierungen oder aufsichtsrechtlich genehmigter Verhaltensregeln erfolgen. Ein besonderes Augenmerk wird in Zukunft auf die Vertragsgestaltung gelegt. Gemäß DSGVO muss ein Datenverarbeitungsvertrag bestimmte Mindestinhalte enthalten, die teils sehr formalisiert sind. In Zukunft wird auch die Möglichkeit bestehen, aufsichtsrechtlich genehmigte Standardvertragsklauseln zu verwenden, die für ein Höchstmaß an Rechtsicherheit sorgen sollten. Die grundsätzliche Verantwortung gegenüber betroffenen Dritten verbleibt allerdings beim Verantwortlichen im Sinne der Verordnung. Verstößt der Auftragsverarbeiter hingegen gegen vertragliche Regelungen oder Weisungen des Verantwortlichen, indem er die Daten zum Beispiel für eigene Zwecke verarbeitet, gilt er gemäß DSGVO selbst als Verantwortlicher – mit allen rechtlichen Folgen. Dazu zählt auch die Pflicht zur Erfüllung der Betroffenenrechte (siehe Grafik unten). In einem solchen Fall haftet auch ein Auftragsverarbeiter in Zukunft gesamtschuldnerisch neben dem Verantwortlichen.

Informieren und Auskünfte geben

Die Ausweitung und Präzisierung der eben erwähnten Betroffenenrechte sind das eigentliche Kernstück der Neuerungen. Die neue Verordnung beinhaltet sowohl eine Ausweitung der Informationspflichten des Verantwortlichen bei Erhebung der Daten als auch der Auskunftsrechte von Betroffenen. Betroffenen steht künftig ein abgestuftes Auskunftsrecht zu. Zunächst kann eine betroffene Person eine Bestätigung darüber verlangen, ob über sie personenenbezogene Daten verarbeitet werden. Eine Negativbescheinigung ist auch in Fällen abzugeben, in denen keine Daten verarbeitet oder diese unumkehrbar anonymisiert wurden. Wurden hingegen personenbezogene Daten verarbeitet, ist über einen umfangreichen Katalog von Informationen (z.B. Datenquellen, Verarbeitungszwecke, Speicherdauer, Löschungsrechte) Auskunft zu geben und Kopien der Daten müssen bereitgestellt werden. Diese Auskunft unterliegt Formvorschriften und muss innerhalb eines Monats auf Kosten des Verantwortlichen erteilt werden. Erleichterungen sind lediglich bei offensichtlich unbegründeten oder exzessiven Anträgen oder bei großen Datenmengen vorgesehen.

Kunden haben künftig ein ausdrückliches „Recht auf Vergessenwerden“ – sämtliche Daten müssen dann gelöscht werden

Darüber hinaus wird neben den bisher bestehenden Widerspruch- und Löschungsrechten jetzt erstmals auch ein ausdrückliches „Recht auf Vergessenwerden“ gesetzlich eingeführt. Bei einem berechtigten Löschungsantrag muss der Verantwortliche dann weitere Verantwortliche, die diese Daten noch verarbeiten, darüber informieren, dass der Betroffene die Löschung der veröffentlichten Daten verlangt. Hierzu sind unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten angemessene Maßnahmen zu treffen.

Bußgelder in Millionenhöhe

Neben den bereits bekannten Aufsichtsinstrumentarien (Verbote, Beschränkungen, Untersuchungsbefugnisse), die sich in Zukunft nicht nur gegen den Verantwortlichen, sondern auch gegen Auftragsverarbeiter richten können, zeichnet sich die Verordnung durch ein verschärftes Bußgeldregime aus. Die Aufsichtsbehörden können jeweils zusätzlich oder anstelle der üblichen Aufsichtsmaßnahmen Verstöße mit Geldbußen ahnden. Der Bußgeldrahmen wird im Grundfall auf bis zu 10 Millionen Euro beziehungsweise bei Unternehmen bis zu 2,0 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres erhöht – maßgeblich ist jeweils der höhere Betrag. Hier gilt ein funktioneller Unternehmensbegriff. Das bedeutet: Der Umsatz der gesamten Unternehmensgruppe wird zur Bußgeldbemessung herangezogen. In besonders schwerwiegenden Fällen verdoppeln sich die Höchstsätze sogar noch auf bis zu 20 Millionen Euro beziehungsweise 4,0 Prozent des Jahresumsatzes. Für die Zumessung gilt der Grundsatz, dass Geldbußen wirksam, verhältnismäßig und abschreckend zu sein haben. Zum Zwecke der europaweit einheitlichen Handhabung von Bußgeldern und Aufsichtsmaßnahmen soll der eingesetzte Europäische Datenschutzausschuss Anwendungsleitlinien erlassen.

Regulatorische Unsicherheiten drohen

Die DSGVO enthält im Vergleich zur bisherigen Rechtslage nachhaltige Verschärfungen – insbesondere die Ausweitung der Betroffenenrechte und die Anhebung des Bußgeldrahmens. Grundsätzlich zur Schaffung eines rechtssicheren europäischen Datenbinnenmarktes geeignet, zeigen sich allerdings bereits vor Inkrafttreten erste Schwierigkeiten. Von den 28 EU-Mitgliedsländern haben trotz zweijähriger Übergangsfrist bis Ende März lediglich zwei (Deutschland und Österreich) ihre nationalen Regelungswerke entsprechend angepasst. Branchenvertreter drängen bereits auf eine befristete Aussetzung der Anwendung der neuen Sanktionsmechanismen. Insbesondere für grenzüberschreitende Finanzdienstleistungen ist daher ab dem 25. Mai 2018 zunächst mit einer regulatorischen Unsicherheitsphase zu rechnen.

Betroffenenrechte nach der europäischen Datenschutz-Grundverordnung (Auswahl) DSGVO, gültig ab 25.05.2018

Artikel	Rechte
13	Informationsrechte (Betroffene müssen informiert werden – u.a. zu Verarbeitungszweck, Weitergabe, Speicherdauer)
15	Auskunftsrechte (Betroffene dürfen Auskunft verlangen – u.a. zu Verarbeitungszweck, Weitergabe, Speicherdauer)
16 u. 21	Berichtigungs- und Widerspruchsrechte
17	Recht auf Löschung und Recht auf Vergessenwerden
21	Recht auf Datenübertragbarkeit

Stand: 13.04.18; Quelle: Otto Mittag Fontane

* Dies ist ein externer Beitrag. Der Inhalt gibt nicht zwingend Meinung und Einschätzung der Redaktion wieder.