Wenn nicht erlaubt, verboten!

Die EU-Datenschutz-Grundverordnung regelt künftig den Umgang mit personenbezogenen Daten. Bei Verstößen drohen drakonische Geldstrafen.

Die neue Datenschutz-Grundverordnung (DSGVO) ist seit Monaten ein Thema für alle Unternehmen in der Europäischen Union, die personenbezogene Daten verarbeiten – und dazu zählen natürlich insbesondere die Finanzdienstleister.

Das gilt nicht nur für Google und Facebook: Kundendaten sind für Unternehmen viel wert. Die gesetzlichen Vorgaben, wie mit diesen Daten umzugehen ist, hinken diesem Umstand jedoch seit Jahren hinterher. Das soll sich ab diesem Jahr ändern. Ab dem 25. Mai tritt nämlich die EU-Datenschutz-Grundverordnung (DSGVO) in Österreich in Kraft. Die DSGVO ist direkt anwendbar und schafft EU-weit einheitliche Datenschutzbedingungen. Viele Betriebe und Unternehmen sind aufgrund der gravierenden Neuerungen verunsichert. Und das zu Recht, denn mangelhaftes Wissen könnten sie bei diesem Thema teuer zu stehen kommen – nicht nur wegen der teilweise drakonischen Geldstrafen, die bei Verstößen drohen.

Mehr Transparenz

Die neuen Regeln verpflichten die Unternehmen zu mehr Transparenz im Umgang mit Kundendaten, wobei dies nun EU-weit einheitlich geregelt ist. Noch gibt es in den EU-Staaten so viele unterschiedliche Datenschutzregelungen wie Mitgliedsstaaten. Mit dem Inkrafttreten der DSGVO wird dies weitgehend vereinheitlicht. Der hohe Datenschutzstandard gilt dann für alle 500 Millionen EU-Bürger und schafft damit gleiches Recht für alle. Die Grundintention des europäischen Gesetzgebers besteht darin, die Privatsphäre des Einzelnen zu schützen. Mit dem technischen Fortschritt geht eine wahre Datenexplosion einher, unglaubliche Datenmengen werden heute bewusst – aber auch unbewusst – verarbeitet. Jedes Unternehmen, das personenbezogene Daten erfasst, ist von der DSGVO betroffen und steht vor der Herausforderung, die neuen Vorgaben in der Praxis erfüllen zu müssen.

Zu den entscheidenden Neuerungen der DSGVO gehört, dass Unternehmen und ihre Dienstleister Rechenschaft darüber ablegen müssen, wie personenbezogene Daten in ihren Systemen verarbeitet werden. Mit der DSGVO soll dabei der Umgang mit personenbezogenen Daten auf ein neues Schutzniveau gehoben werden. Dies reicht von adaptierten Zulässigkeitsvoraussetzungen der Datenverarbeitung über Änderungen im Bereich der Betroffenenrechte bis hin zu erhöhten Informations- und Meldepflichten. Unternehmen haben somit einen erheblichen Mehraufwand und eine große Verantwortung, um den komplexen Anforderungen der DSGVO gerecht zu werden. In der Folge sollen wichtige Neuerungen kurz zusammengefasst werden:

1. Der Schutz personenbezogener Daten wird ausgeweitet:

Um die Anforderungen der DSGVO in Bezug auf das Verarbeiten personenbezogener Daten zu erfüllen, sind entsprechende technische und organisatorische Maßnahmen und Verfahren einzuführen. Zusätzlich muss sichergestellt sein, dass nur die tatsächlich notwendigen personenbezogenen Daten verarbeitet werden. Der Begriff des „Verarbeitens" ist nach der DSGVO weit gefasst. Erfasst ist jeglicher Umgang mit personenbezogenen Daten wie das Erheben, das Speichern, das Auslesen, die Weitergabe, das Verknüpfen, die Organisation, das Ordnen, das Anpassen und auch das Verändern der Daten.

2. Informationspflichten gegenüber Kunden:

Die DSGVO sieht umfangreiche Informationspflichten und Betroffenenrechte vor. Jeder hat das Recht, über die ihn betreffenden gespeicherten und verarbeiteten Daten informiert zu werden. Die Unternehmen müssen auf Wunsch des Kunden unverzüglich (spätestens innerhalb eines Monats) Auskunft über gespeicherte und verwendete Daten geben können. Diese Auskunft hat eine Kopie der Daten – etwa E-Mails, Briefe, Auszüge aus Datenbanken und dergleichen, die Verarbeitungszwecke –, die Kategorien der Daten und die Empfänger oder die Kategorie von Empfängern, die Daten erhalten haben oder erhalten werden, zu beinhalten. Außerdem hat jeder Kunde ein Recht auf „Vergessenwerden": Auf Verlangen sind alle relevanten persönlichen Daten zu löschen.

3. Dokumentations- und Nachweispflichten werden verschärft:

Die DSGVO schreibt vor, dass ein internes Verzeichnis von Verarbeitungstätigkeiten geführt werden muss. Dieses muss nach personenbezogenen Daten, Zweck, Kategorie der betroffenen Person, Empfänger der Daten, Speicherdauer sowie nach den technischen und organisatorischen Maßnahmen zur

Datensicherheit eingeteilt sein. Das Einhalten dieser Dokumentationspflichten muss gegebenenfalls nachgewiesen werden.

4. Risikobewertungen und Datenschutz-Folgenabschätzung:

Sofern mit der Datenverarbeitung ein erhöhtes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen verbunden ist, müssen die Folgen der Datenverarbeitung vorab abschätzbar sein. Darunter fällt etwa das Verarbeiten besonderer Informationen wie etwa Gesundheitsdaten.

5. Was passiert, wenn was passiert?

„Data Breach" ist ein Vorfall, bei dem Unbefugten Zugriff auf persönliche Daten möglich wird, zum Beispiel durch einen Hackerangriff. In einem solchen Fall muss die Meldung an die Aufsichtsbehörde unverzüglich, das heißt innerhalb von 72 Stunden nach Bekanntwerden der Verletzung, erfolgen. Darüber hinaus ist jede betroffene Person zu verständigen.

6. Wann wird ein Datenschutzbeauftragter benötigt?

Besteht die Kerntätigkeit eines Unternehmens in der Verarbeitung personenbezogener Daten (zum Beispiel Profiling, Standort-Tracking, Kundenbindungsprogramme) oder werden sensible Daten (Religion, sexuelle Ausrichtung, Gesundheitsinformationen) verarbeitet, muss ein Datenschutzbeauftragter eingesetzt werden. Das kann ein Mitarbeiter des Unternehmens oder ein externer Experte sein. Dieser kontrolliert, ob die datenschutzrechtlichen Vorschriften und die internen Datenschutzstrategien eingehalten werden.

7. Strafen in Millionenhöhe sind möglich:

Unternehmen, die diese und die sonstigen Regeln der DSGVO nicht einhalten, drohen Strafen in der Höhe von bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorherigen Geschäftsjahres, wobei hier der höhere Wert gilt.

Verboten, was nicht erlaubt ist

Unter dem Regime der DSGVO ist folgender Grundsatz zu beachten: „Es ist verboten, was nicht erlaubt ist." Dies bedeutet, dass die Verarbeitung von personenbezogenen Daten einer Rechtsgrundlage bedarf, etwa einer ausdrücklichen gesetzlichen Erlaubnis oder der Einwilligung der betroffenen Person. Die DSGVO richtet sich dabei vorrangig an jenen, der die Verarbeitung der personenbezogenen Daten verantwortet, daher an denjenigen, der über das Was (Zweck) und das Wie (Mittel) der Verarbeitung entscheidet. Ob diese Verantwortung beim Wertpapierunternehmen oder (zur Gänze) auch beim Wertpapiervermittler liegt, ist im Einzelfall zu prüfen.

Dabei ist zu beachten, dass der Geltungsbereich der DSGVO nicht nur Konsumentendaten umfasst, sondern sich auf die Daten aller natürlichen Personen erstreckt. Für Wertpapiervermittler bedeutet dies, dass auch dann, wenn es sich bei Kunden um Unternehmen handelt, das unmittelbare Gegenüber stets eine natürliche Person ist, die den Schutz der DSGVO genießt.

In der Praxis besonders relevant ist der Aspekt der Datensicherheit. Vor allem wenn Smartphones und Tablets zur Datenverarbeitung eingesetzt werden, ist besonderes Augenmerk auf die IT-Infrastruktur zu legen. Einfach umzusetzen sind noch etwa Maßnahmen, wie jene Geräte, die der Wertpapiervermittler für seine Tätigkeit nutzt, mit Passwörtern oder PIN zu schützen. Der Wertpapiervermittler sollte aber auch stets auf dem aktuellen Stand der Technik bleiben, um die Sicherheit der Daten zu gewährleisten. Das bedeutet, bei PCs und mobilen Endgeräten regelmäßig Programm-Updates durchzuführen, Virenscanner zu verwenden und die Daten regelmäßig zu sichern. Diese Backups sind wiederum sicher aufzubewahren. Bei den verwendeten Programmen ist darauf zu achten, dass diese mit den Vorgaben der DSGVO kompatibel sind. So muss etwa bei Lösungen für Kundendatenbanken darauf geachtet werden, dass die Daten des Kunden gegebenenfalls gelöscht werden können (auch aus den Backups). Andernfalls wird man dem Ersuchen eines (ehemaligen) Kunden, ihn zu „vergessen", nicht nachkommen können (siehe auch Checkliste zu den fünf wichtigsten Grundsätzen bei der Verarbeitung personenbezogener Daten im Kasten unten).

Es bleibt abzuwarten, wie die mitunter neuen und teilweise gestärkten Rechte bei den Verbrauchern ankommen und ob diese davon verstärkt Gebrauch machen werden. Eine kürzlich veröffentlichte Studie zeigt aber, dass eine große Mehrheit der Verbraucher in der EU ihre Rechte auch tatsächlich ausüben möchte. FP

*Die Autoren **Mag. Christian Lenz,** Rechtsanwalt, und **Mag. David Zlabinger,** Rechtsanwaltsanwärter, arbeiten bei der auf Kapitalmarktrecht spezialisierten Kanzlei Brandl & Talos Rechtsanwälte GmbH. Die Kanzlei bietet auch rechtliche Schulungen für Anlageberater an.*

Checkliste für das Verarbeiten von Daten

1. Daten dürfen erst verarbeitet werden, nachdem die betroffene Person dazu eingewilligt hat. Eine Datenverarbeitung hat nach dem Grundsatz der Rechtmäßigkeit zu erfolgen. Das heißt, dass die Verarbeitung auf Basis einer Einwilligung, einer Vertragsanbahnung, einer rechtlichen Verpflichtung oder zum Schutz lebenswichtiger Interessen sowie nach den Grundsätzen von Treu und Glauben (somit fair) und transparent für die betroffene Person zu erfolgen hat.

2. Jede Verarbeitung bedarf eines im Vorhinein festgelegten und eindeutig zuordenbaren Zwecks.

3. Nach Möglichkeit sollten so wenige Daten wie möglich verarbeitet werden. Dem liegt der Grundsatz der Datenminimierung zugrunde. Die Daten dürfen somit nur im unbedingt erforderlichen Ausmaß und nicht länger als für die Zweckerreichung notwendig gespeichert werden.

4. Die Daten müssen vertraulich behandelt werden. Wie auch schon bisher gilt der Grundsatz der Richtigkeit, der Integrität und der Vertraulichkeit der Daten. Es dürfen nur sachlich richtige Daten verarbeitet werden. Personenbezogene Daten sind zusätzlich vor unbefugter oder unrechtmäßiger Verarbeitung und/oder vor Verlust und Zerstörung zu schützen.

5. Eine rechtsgültige Einwilligungserklärung des Kunden ist notwendig. Diese setzt voraus, dass die betroffene Person vom Verantwortlichen in leicht verständlicher und leicht zugänglicher Form sowie in einfacher und klarer Sprache über die Datenverarbeitung aufgeklärt wurde. Dazu muss nachweislich auf den Zweck und die Dauer der Verarbeitung sowie auf die Möglichkeit des Widerrufs der Einwilligung hingewiesen werden.

Quelle: Brandl & Talos