Datenschutzgrundverordnung

Am 25. Mai 2018 tritt die Datenschutzgrundverordnung in Kraft. Sie wird, für manche überraschend, auch als Entbürokratisierungsprojekt angepriesen. Die Autoren sind stolz darauf, in einer für europäische Verhältnisse relativ kurzen Verordnung einige Prinzipien für den Umgang mit personenbezogenen Daten formuliert zu haben. Es soll nicht wie bei der MiFID II hunderte Seiten von Delegierten Rechtsakten geben, vielmehr soll es bei den Prinzipien der unmittelbar geltenden Verordnung bleiben. In einer Art Beweislastumkehr sollen die Unternehmen und Verantwortlichen den Aufsichtsbehörden gegenüber dokumentieren, dass sie compliant sind und diese Prinzipien umgesetzt haben.

Die Prinzipien für den Umgang mit personenbezogenen Daten sind in Artikel 5 der Datenschutzgrundverordnung niedergelegt. Personenbezogene Daten müssen auf rechtmäßige Weise nach Treu und Glauben verarbeitet werden. Sie dürfen nur für legitime Zwecke erhoben und verwendet werden und nicht zu anderen Zwecken weiterverarbeitet oder gar verkauft werden. An dieser Stelle lässt die aktuelle Debatte um die Facebook-Daten grüßen! Es gilt das Gebot der Datenminimierung und Datensparsamkeit, personenbezogene Daten sollen korrekt sein und bei Bedarf berichtigt werden. Die Speicherdauer soll auf das notwendige Minimum reduziert sein. Letztlich sollen personenbezogene Daten vor unbefugter Verarbeitung, Verlust und Zugriff geschützt werden.

Rechtmäßig ist die Verarbeitung von Daten dann, wenn eine Einwilligung der betroffenen Person zur Verarbeitung ihrer Daten vorliegt, die Verarbeitung für die Erfüllung eines Vertrages notwendig ist oder aber zur Erfüllung einer anderen rechtlichen Verpflichtung. Das dürfte für die meisten Vermögensverwalter und Banken die kleinste Hürde sein, denn bereits nach den gesetzlichen Vorgaben des Geldwäschegesetzes und des Wertpapierhandelsgesetzes sind die Institute verpflichtet, größere Mengen von Daten ihrer Kunden zu erfassen, zu speichern und solange die Archivierungsfristen für die Aufsichtsbehörden laufen, aufzuheben. Erfasst daher ein Vermögensverwalter oder Anlageberater die Daten aus dem WpHG-Bogen des Kunden (Anlageziele, Kenntnisse und Erfahrungen sowie die finanziellen Verhältnisse), gestattet ihm das Wertpapierhandelsgesetz dieses ausdrücklich, genauso wie das Geldwäschegesetz die Erfassung, Verarbeitung und Speicherung der Kundenstammdaten sowie des wirtschaftlich Berechtigten erfordert.

Schwieriger wird es, wenn diese Daten nicht nur für die genannten gesetzlichen Zwecke aufgehoben werden, sondern damit auch andere Zwecke verfolgt werden, wie z.B. Marketing, Werbung oder sogar eine Weiterleitung an Konzerngesellschaften zu anderen Zwecken. Dazu wird meistens keine gesetzliche Ermächtigung vorliegen. Dann hilft nur eine Einwilligung des Kunden. Aus unserer Sicht ist es ratsam, sich solche Einwilligungen umfassend einzuholen, am besten gleich in dem Vermögensverwaltungsvertrag, den Rahmenverträgen oder anderen Vertragswerken mit dem Kunden. Dazu sind Formvorschriften der Datenschutzgrundverordnung zu beachten, z.B. das sogenannte Koppelungsverbot. Die Erklärungen sollen in klarer und einfacher Sprache erfolgen und von anderen Sachverhalten in den Dokumenten klar zu unterscheiden sein, ebenso freiwillig und jederzeit widerrufbar. Dazu ist auch ein elektronisches Format zulässig. Zu beachten sind aber die strengen Grenzen der Rechtsprechung, z.B. sollen solche Erklärungen nicht durch bereits vorab angeklickte Checkboxen eingeholt werden. Teilweise wird sogar ein sogenanntes Double-Opt-in-Verfahren verlangt, z.B. für Neukunden auf der Homepage, sie sollen zusätzlich einen per Email übersandten Link anklicken und damit ihr Einverständnis noch einmal bestätigen.

Umfangreicher als bis heute werden die Informationspflichten. Vor Erhebung seiner Daten soll der Betroffene sehr umfassend zu der Verarbeitung seiner Daten informiert werden. Es sind ihm Namen und Kontaktdaten der Verantwortlichen, die Empfänger seiner Daten, die Zwecke der Verarbeitung und Speicherung, seine Rechte zur Auskunft, Löschung, Berichtigung und Datenübertragung sowie auch sein Beschwerderecht mitzuteilen. Dazu wird jedes Institut eine sehr umfassende Datenschutzpolicy entwickeln und zumindest auf seiner Homepage veröffentlichen müssen.

Dem Betroffenen stehen sehr umfassende Rechte gegenüber dem Datenverarbeiter zur Verfügung. Zunächst hat er ein Auskunftsrecht und es muss ihm mitgeteilt werden, welche Daten von ihm verarbeitet und gespeichert worden sind. Er hat das Recht auf Löschung seiner Daten, das berühmt gewordene „Recht auf Vergessenwerden". Dadurch soll der Kunde vor Datenkraken wie Facebook und anderen sozialen Netzwerken geschützt werden. Das gilt aber auch für einen Vermögensverwalter oder eine Bank. Wenn die Daten aufgrund entgegenstehender gesetzlicher Pflichten, wie z.B. den Aufbewahrungspflichten für die Aufsichtsbehörden oder für steuerliche Zwecke, nicht gelöscht werden dürfen, müssen die Daten bei einem Löschungsantrag des Kunden gesperrt werden, so dass sie nicht mehr genutzt oder weiterübermittelt werden können. Der Kunde hat auch das Recht auf Datenübertragung, macht er dieses geltend, müssen ihm seine Daten in einer maschinenlesbaren Form zur Verfügung gestellt werden, damit er mit diesen Daten zu einem anderen Anbieter wechseln kann.

Für die „Robos" wird das Recht auf menschliche Entscheidung relevant. Der Kunde hat das Recht auf nicht nur automatisierte Verarbeitung seiner Daten, wenn eine Entscheidung ihm gegenüber rechtliche Wirkung entfaltet. Dadurch sollen Auswüchse und Missbräuche beim sogenannten „Profiling" vorgebeugt werden. Der Gesetzgeber will erreichen, dass z.B. eine Bank nicht nur auf Basis von gekauften Bewegungsdaten Rückschlüsse auf den gewöhnlichen Aufenthaltsort des Kunden zieht und ihm dann auf Basis eines Algorithmus z.B. einen Kredit verweigert, weil er sich in Gegenden herumgetrieben hat, in denen sich ordentliche Schuldner nicht aufhalten. Das Prinzip gilt auch in der Vermögensverwaltung: Wenn der Kunde lediglich über eine Homepage seine Daten aus dem WpHG-Bogen eingibt und ihm dann ein Algorithmus Anlagerichtlinien unterbreitet und auf Basis dieses Algorithmus eine Vermögensverwaltung durchgeführt wird, erfolgt die Vermögensverwaltung ausschließlich auf Basis automatisierter Verarbeitung. Das muss sich der Kunde nicht gefallen lassen, dazu ist eine ausdrückliche Einwilligung erforderlich, einschließlich einer Beschreibung für den Kunden, wie der Algorithmus seine persönlichen Daten verwendet. Solche Verfahren ziehen auch die Pflicht zu einer aufwendigen Datenschutzfolgeabschätzung nach sich.

Daneben enthält die Datenschutzgrundverordnung Vorgaben an die IT-Ausstattung, die technisch auf der Höhe der Zeit sein muss. Daneben sollen technische und organisatorische Maßnahmen treten, um die Ziele der Datenschutzgrundverordnung zu erreichen. Zum Beispiel wird die Übersendung personenbezogener Daten durch offenen Emailverkehr schwierig, wahrscheinlich wird man Systeme zur Pseudonymisierung oder Verschlüsselung einsetzen müssen. Privacy by Design und Privacy by Default sind hierbei die Stichworte der aktuellen Diskussion.

Lästig sind vor allen die Meldepflichten. Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, soll der Verantwortliche binnen 72 Stunden an die Datenschutzbehörde melden, welche Daten von welchen Personen aufgrund welcher

Schwachstelle verloren gegangen sind. Das sind auch Fälle des im Zug liegen gelassenen Laptops oder des verlorenen USB-Sticks. Dabei drohen Reputationsrisiken, weil auch die Betroffenen von dem Datenleck informiert werden sollen.

Neben diesen allgemeinen Themen existieren natürlich noch Spezialthemen, wie z.B. zum Beschäftigten-Datenschutz und dem Umgang mit sensiblen Daten, wie z.B. Lebensläufen, Krankmeldungen, persönlicher Einschätzung der Führung von Mitarbeitern, etc.. Diese sensiblen Daten sind besonders zu schützen. Es stellen sich aber auch ganz praktische Fragen, wie z.B. ob die private Nutzung dienstlicher Handys noch erlaubt sein soll. Sind diese Geräte nämlich an einen Server des Instituts gekoppelt, werden sensible Daten der persönlichen Kommunikation plötzlich auf Firmenservern gespeichert und kein Datenschutzbeauftragter weiß eigentlich genau, welche Daten von welchen Personen gespeichert und verarbeitet werden. Das beginnt bei Krankmeldungen über WhatsApp an den Chef und endet beim privaten Liebesgesäusel über einschlägige Chats, die sich plötzlich auf dem Firmenserver finden.

Mit den besten Grüßen

Ihr
Dr. Christian Waigel
Rechtsanwalt