DSGVO ist jetzt Pflicht

Das Datenschutzrecht in Europa hat einen langen Weg hinter sich. Das bisher geltende Bundesdatenschutzgesetz gründete im Wesentlichen auf der EU-Datenschutzrichtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr von 1995. Diese gab exakt das Schutzniveau vor, welches die Mitgliedstaaten zu gewährleisten haben. Sie musste durch die jeweiligen Gesetzgeber der Mitgliedstaaten im nationalen Recht verankert werden. Was als Mittel zur Harmonisierung innerhalb der nationalen Datenschutzgesetze in Europa sinnvoll war, erzeugte aber in der Umsetzung einen rechtlichen Flickenteppich, der zur Einheitlichkeit der europaweiten Datenschutzvorschriften nur bedingt beitragen konnte.

Rechtsanwalt Stefan Winheller

Um diese Fragmentierung des Datenschutzrechts in Europa aufzuheben und in der Bestrebung, personenbezogene Daten unter einen noch effektiveren Schutz zu stellen, hat die EU die neue Datenschutzgrundverordnung (DSGVO) erlassen. Sie gilt ab heute unmittelbar in allen Mitgliedstaaten. Als Besonderheit der DSGVO geben einzelne Artikel, sogenannte Öffnungsklauseln, dem nationalen Gesetzgeber die Möglichkeit, von den Vorgaben der DSGVO abzuweichen, wodurch der durch die Verordnung vorgegebene Schutz zwar nicht unterschritten

werden darf, jedoch in einzelnen Bereichen ergänzende und konkretisierende Regelungen getroffen werden können. Diese Freiräume hat der deutsche Gesetzgeber durch das neue Bundesdatenschutzgesetz (BDSG) im Juli 2017 genutzt. Ab Mai 2018 regelt damit das neue BDSG zusammen mit der DSGVO den Datenschutz in Deutschland. Die alten Regelungen, insbesondere auch das bislang gültige Bundesdatenschutzgesetz, werden zeitgleich aufgehoben.

Was sind die wichtigsten Änderungen für Stiftungen?

Bisher im BDSG bestehende die Spendenwerbung privilegierende Vorschriften entfallen. Die DSGVO stellt nämlich den „risikobasierten Ansatz“ als maßgebliche Zulässigkeitserwägung dar, wonach bei der


Rechtsanwältin Nikola Werry

rechtlichen Einschätzung der Zulässigkeit von Werbung auf die „berechtigten Erwartungen“ des jeweiligen Betroffenen abzustellen ist. Diese Wertungsfrage alleine stellt Rechtsanwender vor immense Unsicherheiten.

Hinzu treten eine Vielzahl von Transparenz- und Informationspflichten. Besonders ins Gewicht fällt dabei die Verpflichtung, dass nun Mitglieder, Beschäftigte und Spender deutlich umfassender als bisher über die Verarbeitung ihrer personenbezogenen Daten und die Möglichkeiten zur Ausübung ihrer Rechte informiert werden müssen.

Die DSGVO legt einen restriktiven Ansatz im Umgang mit personenbezogenen Daten fest. Dies führt dazu, dass insbesondere bei den Anforderungen an eine Einwilligung hohe Hürden aufgestellt werden. Unter anderem müssen Einwilligungsklauseln vereinbar mit AGB-Recht sein, das heißt, sie dürfen z.B. nicht überraschend oder missbräuchlich sein. Daneben sind sogenannte Pauschaleinwilligungen unwirksam: Die Einwilligung muss sich also auf einen konkreten Fall beziehen, und sie muss zudem freiwillig gegeben werden. Dies ist nur dann der Fall, wenn die einwilligende Person eine „echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“.

Der Verantwortliche, also die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung entscheidet, hat die Einwilligung nachweisbar zu dokumentieren. Daneben müssen dem Einwilligenden alle Informationen gegeben werden, die mit Art, Umfang und Reichweite der Einwilligung zu tun haben. Betroffene sind außerdem umfangreicher als bislang über ihre Rechte zu informieren, Angaben über die Speicherdauer müssen zur Verfügung gestellt werden. Es braucht hierfür auch ein System, um zu entscheiden, wie lange bestimmte personenbezogene Daten aufbewahrt werden dürfen.

Neue interne Organisationspflichten und IT-Anforderungen

Gravierend wirken sich außerdem – neben der Erforderlichkeit, Einwilligungen sorgsam zu dokumentieren – die internen Organisationspflichten aus, die durch Artikel 5 DSGVO geschaffen werden. Selbst kleine Organisationen müssen danach nicht nur die neuen Pflichten einhalten, sondern auch umfassend dokumentieren, dass diese Pflichten eingehalten werden. Im Kern müssen damit Datenschutzmanagementsysteme geschaffen werden, die in der Lage sind, jeden datenschutzrechtlich relevanten Vorgang umfassend zu dokumentieren und datenschutzrechtliche Compliance (z.B. die Verarbeitung personenbezogener Daten), die Zweckbindung und geeignete technische und organisatorische Maßnahmen nachzuweisen („Rechenschaftspflicht“).

Seitens der IT sind insbesondere spezielle Sicherheitsanforderungen einzuhalten. Datenschutz muss außerdem schon bei der Planung neuer Verarbeitungsvorgänge durch die Vornahme datenschutzrechtlicher Grundeinstellungen und bei der Entwicklung neuer Geräte durch datenschutzfreundliche Konzeption berücksichtigt werden („privacy by default“ und „privacy by design“).

Besonders an der DSGVO ist auch, dass sie die sogenannte Datenschutz-Folgenabschätzung (DSFA), einführt. Im Grundsatz ist diese vergleichbar mit der nach bisher gültigem Datenschutzrecht vergleichbaren Vorabkontrolle – mit dem Unterschied, dass zu erwarten ist, dass der DSFA im Vergleich zur Vorabkontrolle durch die rechtliche Ausgestaltung ein größerer Anwendungsbereich zukommt. Eine DSFA ist immer dann vorzunehmen, wenn „(…) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge (hat)“.

Die Idee dahinter ist schnell ersichtlich: Verantwortliche sollen sensibilisiert bleiben für die Rechte der Betroffenen und die relevanten Prozesse und Vorgänge ständig überprüfen. Mögliche Risiken bei bestimmten Datenverarbeitungen sollen dadurch bewusster behandelt und datenschutzrechtlich möglicherweise problematische Prozesse von vornherein besser evaluiert werden.

Ab heute ist Compliance unbedingt erforderlich

Bis heute mussten alle erforderlichen Umsetzungsmaßnahmen ergriffen und abgearbeitet sein. Herausfordernd ist dies nicht nur deshalb, weil sich nun, nachdem auch der nationale Gesetzgeber entsprechend reagiert hat, insbesondere Fachkreise und Datenschutzbehörden erst nach und nach positionieren werden, was bei der Auslegung und Anwendung der relevanten Vorschriften zu beachten ist.

Fest steht schon jetzt, dass Verstöße gegen die DSGVO strenger geahndet werden als bislang. Neben den aktuell auch bestehenden Ansprüchen auf zivilrechtlichen Schadensersatz und strafrechtliche Verfolgung sind die zu erwartenden Bußgelder empfindlich gestiegen und können im Ernstfall bis zu 20 Millionen Euro oder auch vier Prozent des weltweit erzielten Jahresumsatzes betragen – je nachdem, welcher Betrag höher ist. Und das will ja nun wirklich niemand.

Über die Autoren:
Stefan Winheller ist Gründer und Managing Partner der Kanzlei Winheller. Als Fachanwalt für Steuerrecht berät er hauptsächlich gemeinnützige Organisationen und Unternehmen am

Hauptsitz in Frankfurt am Main.

Nikola Werry leitet die Praxisgruppe IP/IT und Datenschutz bei der auf das Gemeinnützigkeitsrecht spezialisierten Kanzlei Winheller. Sie ist Gastdozentin für E-Commerce und IT-Recht an der Universität Passau.

Dieser Beitrag erschien in DIE STIFTUNG **5/2017.**