DSGVO – fünf Buchstaben, die Arbeit machen

Carsten J. Diercks, Rechtsanwalt, Politikberater und langjähriger rechtlicher Berater der DOAG

Vom 25. Mai 2018 und seiner Bedeutung für den Datenschutz haben alle bereits gehört. Der Artikel zeigt die gravierenden Änderungen im gewohnten Umgang mit Datenschutz und Datensicherheit auf, die sich durch die neuen Regelungen der Datenschutzgrundverordnung DSGVO ergeben.

Diesmal kann man kaum behaupten, von einer europäischen Regelung überrascht worden zu sein. Die Regierungen der Mitgliedsstaaten im Rat der EU und das Europäische Parlament waren großzügig bei der Bemessung einer Übergangszeit. Bereits seit dem 24. Mai 2016 ist die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG" (DSGVO, englisch GDPR) in Kraft. Am 25. Mai 2018 kommen die Regelungen nun zur Anwendung. Auf Grundlage der in den 1980er-Jahren entstandenen datenschutzrechtlichen Bestimmungen wurde im Jahr 1995 eine erste Generation europäischer Regelungen geschaffen. Nach zwanzig Jahren und angesichts eines gravierend veränderten Umfelds in Technik und Gesellschaft sowie durch Globalisierung war eine Neuregelung notwendig. Zwar ist mit der DSGVO nicht der große Wurf einer wirklichen Reform gelungen, es ergeben sich aber erhebliche Änderungen in der Grundkonstruktion.

DSGVO: europaweit für alle Akteure geltend

Die DSGVO gilt als Verordnung unmittelbar in allen Mitgliedsstaaten der Europäischen Union für datenverarbeitende Behörden und Unternehmen. Eine Umsetzung in den nationalen Rechtsordnungen ist nicht erforderlich. Sie bildet die neue Basis für den Datenschutz und weist starke Bezüge auch zur Datensicherheit auf. Allerdings sind die 99 Artikel und 173 Erwägungsgründe nicht gänzlich abschließend – sie lassen Raum für die Mitgliedsstaaten, diesen auszufüllen und teils auch eigene Regelungen zu treffen. Das Bundesdatenschutzgesetz wird daher daneben als „BDSG-neu" mit reduziertem Anwendungsbereich fortbestehen; ebenso die Landesdatenschutzgesetze und einige spezialgesetzliche Regelungen – so ist etwa der Beschäftigtendatenschutz weiterhin in nationaler Kompetenz.

Am Horizont ist bereits die nächste Regelung erkennbar, die nicht nur zu erheblichen politischen Diskussionen führen, sondern auch für die Wirtschaftswelt Herausforderungen bringen wird: die e-Privacy-Richtlinie, die die EU-Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG ablösen soll und sich beispielsweise auf Cookie-Anwendungen bezieht.

Dies vorausgeschickt, ergibt sich eine im Wesentlichen einheitliche Rechtsordnung in den 28 – und ab 30. März 2019 voraussichtlich 27 – Mitgliedsstaaten. Zwar bleibt es bei nationalen Behörden, komplexe Kooperations- und Kohärenz-Mechanismen sorgen jedoch für eine einheitliche Rechtsanwendung insbesondere bei grenzüberschreitender Datenverarbeitung.

Hat ein Unternehmen mehrere Sitze in der Europäischen Union, ist die Aufsichtsbehörde am Hauptsitz des Unternehmens zuständig, die die Aufsichtsbehörden der anderen Mitgliedsstaaten erforderlichenfalls einbindet. Damit gibt es einen „one stop shop"-Mechanismus, der nicht nur für in der EU ansässigen Unternehmen gilt, sondern auch für nicht ansässige. Es herrscht fortan das Marktort-Prinzip. Die DSGVO gilt also nicht nur für Unternehmen mit einer Niederlassung in der EU, die auch aus einem Briefkasten bestehen kann, sie gilt ebenso für Unternehmen ohne Niederlassung, die Daten von Personen, die sich in der Europäischen Union aufhalten, zum Vertrieb von Waren und Dienstleistungen oder Beobachtung von Verhalten verarbeiten. Anders gesagt, jedes Unternehmen, das in der EU künftig Daten verarbeitet, unterliegt der DSGVO.

Dabei ist zu bemerken, dass sich die DSGVO weiterhin nur auf personenbezogene Daten bezieht; Unternehmens- oder Maschinendaten sind nicht betroffen. Personenbezogen sind alle Daten, die einer lebenden natürlichen Person zugeordnet werden können, sie also identifizierbar machen. Im Zweifel ist also eher von der Personenbezogenheit auszugehen. Im Zentrum aktueller Diskussionen dazu steht die Frage der Identifizierbarkeit bei Big-Data-Anwendungen. Generelle Aussagen sind dazu jedoch kaum möglich und jede Big-Data-Anwendung ist im Einzelnen zu betrachten.

Der risikobasierte Ansatz

Hinsichtlich der personenbezogenen Daten bleibt es bei dem aus dem deutschen BDSG bekannten Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt. Eine Verarbeitung ist also nur möglich, wenn eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt. Die Änderungen ergeben sich hier im Detail: Die DSGVO setzt hier wesentlich mehr auf den sogenannten „risikobasierten Ansatz". An diversen Stellen der Verordnung wird eine Datenverarbeitung im Interesse des Verarbeiters erlaubt, wenn nicht Interessen des Betroffenen überwiegen. Dies führt zu einigen Änderungen, so entfallen das sogenannte „Listenprivileg" des BDSG oder die Regelungen zum Scoring. Letzteres wird in der DSGVO durch die De-

tail-Regelungen zum Profiling ersetzt, die jedoch nur anzuwenden sind, wenn eine Entscheidung mit rechtlicher Wirkung Ergebnis der Verarbeitung sein soll.

Von der DSGVO erfasst wird jede automatisierte Verarbeitung oder die Verarbeitung zur elektronischen Speicherung von personenbezogenen Daten. Ausgenommen sind nur die Verarbeitung zu persönlichen oder familiären Zwecken sowie der strafrechtliche Bereich der öffentlichen Verwaltung. Für den elektronischen Geschäftsverkehr gehen die Regelungen der Richtlinien RL 2000/31/EG und 2011/83/EG für Dienste-Anbieter bei der Durchleitung von Informationen, Zwischenspeicherung und Host-Provider vor. Es werden nicht mehr einzelne Verarbeitungsschritte differenziert, sondern einheitlich der Begriff der Verarbeitung benutzt. Zu den weiteren Begrifflichkeiten sei auf Artikel 4 der DSGVO verwiesen sowie bei den besonders zu schützenden sensiblen, personenbezogenen Daten auf Artikel 9 DSGVO, etwa bei biometrischen Daten, Gesundheitsdaten oder Daten zu politischen Meinungen.

Die DSGVO beschreibt darüber hinaus eine Reihe von Grundsätzen für die Datenverarbeitung. Daten müssen danach auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Treu und Glauben, Transparenz); für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung); dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung); sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Richtigkeit). Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Speicherbegrenzung); in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit).

Neu und eine erhebliche Arbeitslast auf den für die Datenverarbeitung Verantwortlichen ist der Grundsatz der Rechenschaftspflicht. Die DSGVO spricht hier davon, dass sie verantwortlich sind und die Einhaltung der Grundsätze nachweisen können müssen. War es bisher Aufgabe der Aufsichtsbehörden, bei Beschwerden den Verstoß zu belegen, ist es nun weit im Vorfeld die Aufgabe des Verantwortlichen, die Einhaltung der Grundsätze im Einzelnen zu dokumentieren. Dies ist eine Umkehr der Beweislast, die eine der großen Veränderungen durch die DSGVO bedingt.

Der Verantwortliche muss daher seit dem Inkrafttreten die gesamte Datenverarbeitung prüfen, durchdenken und dokumentieren, um möglichen Sanktionen zu entgehen. Die hier in Rede stehenden Summen bis zu zwanzig Millionen oder bis zu vier Prozent des weltweiten Jahresumsatzes sind hinreichend berichtet. Weniger berichtet wird, dass selbst die Datenschutzbeauftragten zugeben, diese Bußen nur in wenigen Fällen verhängen zu können. Eine flächendeckende Aufsicht ist schlichtweg nicht möglich. So wird es zu Maßnahmen gegen Leuchttürme von Branchen kommen, in der Hoffnung, dass dies zu einer breiten Anwendung der DSGVO beiträgt. Wer allerdings mit seinem Geschäftsmodell in dem Risiko steht, dass Betroffene sich sehr schnell an die Datenschutzbeauftragten wenden, wird größere Anstrengungen in Compliance investieren müssen. Angesichts der Herausforderungen bei der Implementierung der DSGVO gehen weite Kreise von Datenschutzrechtlern davon aus, dass es kaum ein Unternehmen schaffen wird, zum Stichtag noch beziehungsweise schon wieder compliant zu sein.

Zulässigkeit der Datenverarbeitung

Zurück zur Erlaubnis für die Datenverarbeitung, also der Einwilligung des Betroffenen oder einer gesetzlichen Grundlage. Die Einwilligung wird wie bisher vom Betroffenen erteilt. Sie ist jedoch zum einen widerruflich für die Zukunft ausgestaltet, zum anderen zu ihrer Wirksamkeit an Voraussetzungen geknüpft. Zwar ist keine Schriftform mehr erforderlich, die Einwilligung ist jedoch freiwillig und informiert abzugeben. Einwilligen können Kinder ab 16 Jahren, darunter ist eine Einwilligung oder die Zustimmung der Erziehungsberechtigten erforderlich.

Vor einer Einwilligung muss umfangreich informiert werden. Nach Artikel 13 DSGVO betrifft dies Identität und die Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung, gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und gegebenenfalls zusätzliche Informationen. Dazu hat der Verantwortliche zu informieren über die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer; das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit; über das Recht, die Einwilligung jederzeit zu widerrufen; das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche mögliche Folgen die Nichtbereitstellung hätte und das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. Diese Informationspflichten bestehen auch, wenn die Daten von einem Dritten erhoben werden. Ausnahmen von den Informationspflichten bestehen nur, wenn die Informationen bereits dem Betroffenen bekannt sind.

Eine Menge von Angaben rund um die Einwilligung, deren Übermittlung, aktuelle Fassung etc. neben der eigentlichen Einwilligung ist sorgsam zu dokumentieren, denn gerade in diesem Feld wird die Aufsicht ansetzen. Dies gilt in besonderem Maße für die Fälle, in denen keine Einwilligung vorliegt, sondern die Verarbeitung auf einer gesetzlichen Erlaubnis besteht. Hier macht sich der risikobasierte Ansatz bemerkbar, was insbesondere die Dokumentationspflichten vor der Erhebung angeht. Artikel 6 DSGVO sieht neben der Einwilligung beispielsweise vor, dass eine Verarbeitung rechtmäßig ist, wenn

WIN VERLAG **Kiosk**

30 Tage gratis lesen

Jetzt auch als digitale Ausgabe

Auf 5 Geräten gleichzeitig lesen:
- im Web & per App

Shoppen wie man möchte:
- von Artikel bis Abo

united-kiosk.de/kiosk-win

die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei der Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Betroffenen erfolgen; die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt; die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen oder die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Von besonderer Wichtigkeit ist jedoch die Regelung in Artikel 6 I f), nach dem die Verarbeitung zulässig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen, die den Schutz personenbezogener Daten erfordern, überwiegen; insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Was sich anhört wie ein Sonderfall, wird absehbar neben der Einwilligung der wichtigste Fall werden. Auf diesen werden sich zukünftig weitere Bereiche der Werbung und des Marketings stützen können. Als berechtigtes Interesse des Verarbeiters wird durchaus auch ein eigenwirtschaftliches Interesse verstanden. Die Gründe für die Abwägung mit den Betroffenenrechten müssen aber tragen und dokumentiert sein. Hier wird erheblicher Aufwand erforderlich sein und letztlich die Aufsichts- und Rechtsprechungspraxis die Grenzen definieren.

Der risikobasierte Ansatz ist auch bei den Regelungen zur Zweckänderung erkennbar: Soll eine Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ohne Einwilligung des Betroffenen oder eine rechtliche Erlaubnis erfolgen, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem jede Verbindung zwischen den Zwecken, den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, die Art der personenbezogenen Daten, die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen und das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

Rechte der Betroffenen

Der Verantwortliche für die Datenverarbeitung hat die Interessen des Betroffenen also nicht nur mitzudenken, sondern auch auf die Geltendmachung der in der DSGVO enthaltenen Rechte der Betroffenen einzugehen und angemessen zu reagieren. Der Katalog der Rechte beginnt mit dem Recht auf präzise, transparente, verständliche und leicht zugängliche Information in verständlicher Sprache. Zukünftig werden also schwammige oder nichtssagende Texte vor der Einwilligung nicht mehr zulässig sein, weil sie die Wirksamkeit der Einwilligung gefährden. In diesem Zusammenhang sei darauf hingewiesen, dass die deutschen Datenschutzbeauftragten am 14. September 2016 beschlossen haben, dass vor dem 25. Mai 2018 rechtswirksam erteilte Einwilligungen fortgelten. Schwierig wird hier mitunter der hinreichend dokumentierte Nachweis sein.

Die Betroffenenrechte seien hier nur kurz aufgezählt: Recht auf Information bei Erhebung, bei anderweitiger Erhebung, bei Zweckänderung; Recht auf Auskunft; Recht auf Berichtigung; Recht auf Löschung (Recht auf Vergessenwerden); Recht auf Einschränkung der Verarbeitung (Sperrung); Recht auf Datenübertragbarkeit; Widerspruchsrecht bei besonderer Situation in Fällen der Verarbeitung im öffentlichen Interesse oder bei Abwägung, Profiling oder Direktwerbung und ein grundsätzliches Verbot automatisierter Entscheidungen im Einzelfall, es sei denn, es liegt eine Einwilligung, ein Vertrag oder ein Gesetz vor. Auch dies hat Einfluss auf die zukünftige Gestaltung von Datenverarbeitung, allein was beispielsweise Vergessenwerden oder die Datenübertragbarkeit angeht.

Auftragsverarbeitung, Verarbeitungsverzeichnis, Folgenabschätzung

Nach der Darstellung dieser Grundlagen kann es nun an die Neuerungen in einzelnen Bereichen der Verarbeitung gehen. Ein zentraler Bereich ist nun die Auftragsverarbeitung. Nicht nur die Bezeichnung ist eine neue, auch die Regelungen hierzu sind geändert. So begeben sich Auftragsverarbeiter, die unter Verstoß gegen die DSGVO agieren, in eigene Verantwortlichkeiten. Die Auftragsdatenverarbeitung darf nur auf Grundlage einer vertraglichen Vereinbarung, die auch elektronisch geschlossen werden kann, nach den inhaltlichen Vorgaben der DSGVO erfolgen. Dazu gehören beispielsweise die genaue Beschreibung der Aufgaben des Auftragsverarbeiters und hinreichende Garantien von diesem für angemessene technische und organisatorische Maßnahmen (TOM). Diese TOM-Anforderung gilt damit auch im Bereich des Cloud-Computing. Auch hier wird verlangt, dass der Cloud-Nutzer nur mit Cloud-Anbietern zusammenarbeitet, die hinreichend Garantien dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Bei jeder Art von Cloud-Lösung ist diese Prüfung vorzunehmen, da generelle Aussagen hier kaum möglich sind.

Neu benannt wurde auch das vom BDSG bekannte Verfahrensverzeichnis. Es heißt nun Verarbeitungsverzeichnis und ist bei Verantwortlichen mit mehr als 250 Mitarbeitern Pflicht. Aber auch unterhalb dieses Schwellenwerts kann ein Verzeichnis der Verarbeitungstätigkeiten notwendig werden, wenn die vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten betrifft. Hier ist eine sorgsame Prüfung erforderlich.

Ebenso wurde aus der BDSG-Vorabkontrolle nun eine Folgenabschätzung. Sofern ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, ist diese erforderlich. Dies muss kein finanzieller Schaden sein, es geht auch um Diskriminierung, Identitätsdiebstahl, Rufschädigung, Verlust der Vertraulichkeit, Aufhebung der Pseudonymisierung oder den Verlust der Kontrolle über die eigenen Daten. Das Ergebnis der Risikoanalyse und die daraus resultierenden Maßnahmen sind zu dokumentieren. Gegebenenfalls ist auch die Aufsichtsbehörde zu konsultieren, wenn ein hohes Risiko besteht. Hier sowie bei den Verarbeitungsverzeichnissen können Vorlagen der Aufsichtsbehörden genutzt werden.

Datensparsamkeit und Datensicherheit

Die DSGVO gibt weitere Grundsätze für die Gestaltung der Datenverarbeitung vor: Durch technische und organisatorische Möglichkeiten muss sichergestellt sein, dass der Datenschutz verwirklicht wird. „Privacy by Design“ soll die Verarbeitung so ge-

stalten, dass der Datenschutz bereits in der Grundkonstruktion berücksichtigt ist. „Privacy by Default" soll insbesondere bei Online-Anwendungen sicherstellen, dass bei Vorgaben stets die datenschutzfreundlichste Variante voreingestellt ist. Die Beachtung dieser Grundsätze wird bei der Bemessung von Bußgeldern eine Rolle spielen und ist daher nicht nur ein Selbstzweck.

Artikel 32 der DSGVO beschäftigt sich mit der Verpflichtung zur Datensicherheit, wonach geeignete technische und organisatorische Maßnahmen zu treffen sind, die dem Stand der Technik entsprechen und nach Kosten und Risiko verhältnismäßig sind. Die Datensicherheit betrifft aber auch die Aspekte der weitgehenden Pseudonymisierung, der Sicherstellung der Fähigkeiten von Systemen und Diensten, der Wiederherstellung der Verfügbarkeit und des Zugangs zu Daten sowie von Verfahren zur Überprüfung der Gewährleistung der Sicherheit der Verarbeitung. Auch hier wird die Aufsicht mehr als ein Auge auf den Nachweis der Einhaltung dieser Voraussetzungen haben.

Von Bedeutung ist dabei auch die Festlegung von Prozessen bei Verletzung des Schutzes personenbezogener Daten, also „Unfällen" bei der Sicherheit von Daten. Die DSGVO schreibt vor, dass binnen 72 Stunden nach Kenntnis über einen Verstoß die zuständige Aufsichtsbehörde zu verständigen ist. Hierzu wird es ein Online-Tool bei den Datenschutzbeauftragten geben. Die Meldung kann nur unterbleiben, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hier ist anzuraten, diese Prognose-Entscheidung genau zu dokumentieren.

Sofern mit der Verletzung des Datenschutzes voraussichtlich ein hohes Risiko für den Betroffenen verbunden ist, muss dieser ebenfalls informiert werden. Dies kann unterbleiben, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat, etwa durch Verschlüsselung, oder wenn der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht. Ferner wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. Dies bedeutet für jeden Verantwortlichen, dass er ein Notfall-Management einführen muss, das die notwendigen Prozesse mit den dazugehörigen Verantwortlichkeiten definiert und entsprechende Informationsmaßnahmen vorbereitet.

Zur betrieblichen Organisation gehört ferner in bestimmten Fällen ein Datenschutzbeauftragter, wie er seit dem BDSG bekannt ist. Der Schwellenwert, bei dessen Überschreiten ein Datenschutzbeauftragter einzusetzen und nun auch der Aufsicht zu benennen ist, bleibt bei zehn Personen, die regelmäßig Zugriff auf die personenbezogenen Daten nehmen. Außerdem ist ein Datenschutzbeauftragter zu benennen, unter anderem wenn die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder die Kerntätigkeit im Umgang mit besonders sensiblen Daten liegt. Die Berufung kann auch freiwillig erfolgen. In jedem Fall ist sie aber intern und extern bekannt zu machen.

Schließlich noch ein kurzer Blick auf die Weitergabe von Daten an Dritte. Die Weitergabe innerhalb der Europäischen Union ist weitgehend unproblematisch, da sie als Inland gilt. Die Übermittlung von Daten ist grundsätzlich nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die Bedingungen der DGSVO einhalten. Tragender Gedanke ist, dass das Schutzniveau der DGSVO nicht untergraben werden soll, wie insbesondere in den Erwägungsgründen ausgeführt wird: Die EU-Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Gibt es einen solchen Angemessenheitsbeschluss nicht, sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, auf von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder auf von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Dieses Thema bedarf einer eingehenden Erörterung, insbesondere im Verkehr mit den USA angesichts der „Privacy Shield"-Politik, die den Rahmen dieses Beitrags sprengen würde.

Abschließend stellt sich also die Frage, was zu tun ist, um am 25. Mai 2018 vorbereitet zu sein. Zunächst sollten eine Bestandsanalyse erfolgen und alle Prozesse der Verarbeitung von Daten erfasst werden. Sodann können diese mit einer GAP-Analyse darauf geprüft werden, welche Prozesse noch auf den Stand der DSGVO zu bringen sind. Die notwendigen Abläufe und Prozesse in den Abteilungen sowie in der IT sind anzupassen. Verträge, insbesondere Auftragsdatenverarbeitungsverträge, sind auf den neuen Stand zu bringen. Dies gilt auch für andere rechtlich relevante Dokumente und vor allem für die Informationen bei Einwilligungen. Das Unternehmen sollte ein Leitbild für den Datenschutz entwickeln und Mitarbeitende sowie Führungskräfte auf die DSGVO-Änderungen vorbreiten.

Letztlich bedingt die Anwendbarkeit der DSGVO ab Ende Mai genau das, was der Gesetzgeber intendiert hat: eine intensive Beschäftigung mit dem Thema „Datenschutz" und den Aufbau oder die Überarbeitung der gesamten Datenschutzorganisation in einem Unternehmen. Schon aus den in diesem Beitrag aufgezeigten Punkten ergibt sich ein großer Prüfungs- und Dokumentationsaufwand.

Weiterführende Informationen

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de
- Kranig, Sachs, Gierschmann, Datenschutz-Compliance nach der DS-GVO, Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, 230 Seiten, Verlag Bundesanzeiger, ISBN 978-3846207604, 44 Euro

Carsten J. Diercks
cj@diercksrechtsanwalt.de