Anforderungen und Umsetzung der EU-Datenschutz-Grundverordnung

Rechtsanwalt Dr. Carsten Ulbricht, Bartsch Rechtsanwälte

Ab 25. Mai 2018 gilt europaweit die europäische Datenschutz-Grundverordnung (DSGVO) und löst damit das bisher in Deutschland für den Datenschutz geltende Bundesdatenschutz-Gesetz (BDSG) ab. Im Zusammenwirken mit den Änderungen im nationalen Gesetz durch das BDSG-neu sorgt die Umsetzung der DSGVO wegen der erheblich erhöhten Bußgelder bei zahlreichen Unternehmen derzeit für viel Verunsicherung. Der Artikel erläutert die neuen Anforderungen in möglichst kompakter Form und fasst die wesentlichen Maßnahmen in einem Zehn-Punkte-Plan zusammen.

Mit der Datenschutz-Grundverordnung will die Europäische Union (EU) ein gleich hohes Datenschutz-Niveau innerhalb der EU-Staaten schaffen, die Kontrolle und Transparenz der Verarbeitung personenbezogener Daten stärken und den bisherigen Datenschutz- und Vollzugs-Defiziten durch erheblich erhöhte Bußgelder entgegenwirken. Soweit noch nicht geschehen, sollten die eigenen Datenverarbeitungsvorgänge unmittelbar analysiert und die neuen Anforderungen der DSGVO im Hinblick auf den verbindlichen Stichtag des 25. Mai 2018 unverzüglich umgesetzt werden. Unternehmen, die dies versäumen, riskieren sonst tatsächlich eine Verhängung empfindlicher Bußgelder.

Mit Umsetzung und Dokumentation der nachfolgend erläuterten Maßnahmen lassen sich die wesentlichen Anforderungen jedoch gut erfüllen. Zur leichteren Umsetzung hat die Kanzlei des Autors eine Vielzahl konkreter Hinweise, Checklisten und Musterdokumente zusammengestellt, die dabei helfen sollen, noch rechtzeitig DSGVO-compliant zu werden.

Was die EU-Datenschutz-Grundverordnung regelt

Die DSGVO regelt den Schutz personenbezogener Daten im Sinne von Artikel 4, Absatz 1 DSGVO. Nach dessen Definition sind personenbezogene Daten sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung – wie einem Namen, einer Kennnummer, Standort-Daten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen – identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Nach dieser Definition sind also all die Informationen als personenbezogen anzusehen, die sich über die dem Unternehmen oder Dritten vorliegende Kenntnisse einer natürlichen Person zuordnen lassen. Typische personenbezogene Daten sind daher:

- Name
- Wohnadresse
- Geburtsdatum
- E-Mail-Adresse (auch geschäftliche E-Mail-Adressen wie „vorname.nachname@firma.de")
- Telefonnummer
- Eigenschaften einer Person
- Kundennummer
- Vollständige IP-Adresse
- Online-Kennungen, die eine Zuordnung zu einer Person ermöglichen

Der Anwendungsbereich der DSGVO ist sehr weit gefasst. Sobald ein Unternehmen solche personenbezogenen Daten erhebt, speichert oder verarbeitet, sind die Vorgaben der DSGVO für diese Verarbeitungsvorgänge zu beachten. Ansonsten kann die Verletzung der DSGVO empfindliche Bußgelder nach sich ziehen. Je nach Schwere des Verstoßes können die Aufsichtsbehörden bis zu zwanzig Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes als Bußgeld verhängen. Für leichtere Verstöße ist ein

Bußgeld von maximal zehn Millionen Euro oder von zwei Prozent des weltweiten Jahresumsatzes vorgesehen.

Rechtmäßigkeit

Die DSGVO sieht für die Verarbeitung personenbezogener Daten das sogenannte „Verbotsprinzip" vor. Das bedeutet, dass eine Datenverarbeitung grundsätzlich verboten ist, wenn die konkrete Verarbeitung nicht ausdrücklich von der DSGVO gesetzlich erlaubt wird oder auf der informierten Einwilligung der betroffenen Person beruht.

Soweit im Unternehmen nicht bereits ein Verfahrensverzeichnis als Übersicht über die eigenen Verarbeitungsvorgänge vorliegt, sollten im Rahmen einer Bestandsaufnahme die Vorgänge und Prozesse im Unternehmen zusammengestellt werden, bei denen personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Personenbezogene Daten dürfen im Rahmen dieser Vorgänge und Prozesse zukünftig nur verarbeitet werden, wenn eine der Voraussetzungen des Artikels 6 DSGVO die jeweilige Verarbeitung ausdrücklich legitimiert. Gemäß diesem dürfen Unternehmen in folgenden Fällen Daten verarbeiten:

- Die Daten sind zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme erforderlich
- Der Betroffene willigt auf Grundlage einer informierten Aufklärung ein
- Die Daten werden zur Erfüllung einer rechtlichen Verpflichtung benötigt
- Die Datenverarbeitung ist zur Wahrung berechtigter Interessen des Unternehmens oder eines Dritten erforderlich und die Interessen der betroffenen Person überwiegen nicht

Nach der Bestandsaufnahme sollten Unternehmen für die eigenen Datenverarbeitungsvorgänge (wie E-Mail-Marketing) also prüfen, unter welchem der Legitimations-Tatbestände die jeweilige Verarbeitung (etwa beim E-Mail-Marketing über eine Einwilligung) legitimiert werden kann. Dabei genügt es, wenn die jeweilige Datenverarbeitung unter einen der Legitimations-Tatbestände fällt.

Informationspflicht

Die EU-DGSVO sieht im Interesse der Transparenz der eigenen Datenverarbeitung sehr weitreichende Informationspflichten der Unternehmen vor. Je nachdem, ob die personenbezogenen Daten beim Betroffenen (Artikel 13 DSGVO) oder anderweitig (Artikel 14 DSGVO) erhoben werden, ist der Betroffene gemäß den gesetzlichen Vorgaben zu informieren. Deshalb ist die betroffene Person – in der Regel schon bei der Erhebung – darüber zu informieren, welche Daten das Unternehmen für welchen Zweck verarbeitet, an welche Stellen es die Daten weitergibt oder ob eine Weitergabe beabsichtigt ist. Zudem gibt es umfangreiche Betroffenenrechte (wie Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht), über die die Person ebenfalls zu informieren ist. So ist zum Beispiel für die eigene Webseite beziehungsweise dort stattfindende Erhebungsvorgänge (wie Vertragsschluss, Kontaktformular, Drittanbieter-Werkzeuge) in jedem Fall sicherzustellen, dass die eigene Datenschutzerklärung den differenzierten Anforderungen des Artikels 13 DSGVO genügt.

Technischer Datenschutz

Die DSGVO verknüpft den Datenschutz sehr stark mit der Technik. Deshalb sind bei der Verarbeitung personenbezogener Daten auch konkrete Anforderungen an die Datensicherheit zu erfüllen. IT-Verfahren müssen zudem schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (Privacy by Design/Privacy by Default).

Weitergabe von Daten an Dritte

Zur Anpassung der Datenschutz-Organisation an die neuen Anforderungen der DSGVO gehört es dann auch, bestehende Vertragsverhältnisse auf etwaige Änderungen, die durch die DSGVO erforderlich werden, zu prüfen. Dies gilt allem voran für Verträge zur Auftragsdatenverarbeitung nach § 11 BDSG. Diese dient nach aktueller Rechtslage als Konstruktion, um die Weitergabe personenbezogener Daten seitens eines Verantwortlichen (nachfolgend Auftraggeber) an Dienstleister (nachfolgend Auftragnehmer) innerhalb des europäischen Wirtschaftsraumes datenschutzrechtlich zulässig zu gestalten.

Typische Konstellationen, bei der die Weitergabe an einen Dienstleister über eine Auftragsverarbeitung legitimiert wird, sind die Speicherung von personenbezogenen Daten bei einem Dritten (etwa Kundendaten in der Oracle Marketing Cloud) oder aber auch die Weitergabe an einen E-Mail-Dienstleister (wie MailChimp).

Soweit das Unternehmen also einen Teil der (eigenen) Datenverarbeitung an Dritte ausgelagert hat, sind die mit dem jeweiligen Dienstleister nach § 11 BDSG geschlossenen Verträge zur Auftragsdatenverarbeitung an die neue Rechtslage anzupassen. Diese findet sich in den Artikeln 28 und 29 DSGVO, die den § 11 BDSG ablösen werden. Die DSGVO spricht dann auch nicht mehr von Auftragsdatenverarbeitung, sondern von Auftragsverarbeitung.

Fortan wird also ein entsprechender Auftragsverarbeitungsvertrag nach Artikel 28 Absatz 3 Seite 1 DSGVO die Weitergabe von personenbezogenen Daten legitimieren, ohne dass ein Erlaubnis-Tatbestand nach Artikel 6 Absatz 1 DSGVO vorliegen müsste oder die Einwilligung der betroffenen Person eingeholt worden ist. Auch an dieser Stelle zeigt sich also, dass mit der DSGVO keine komplette Neuregelung verbunden ist, sondern lediglich die auch bisher schon nach dem BDSG geltende Rechtslage an die DSGVO anzupassen ist. Unternehmen können daher ihren bisherigen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG weiter nutzen, haben diesen aber sowohl inhaltlich als auch an die teils geänderten Begrifflichkeiten anzupassen.

Mitverantwortung des Auftragsverarbeiters

Eine wesentliche Änderung ergibt sich aus der Entscheidung des europäischen Gesetzgebers, auch den Auftragsverarbeiter, den Auftragnehmer, stärker in die Pflicht zu nehmen und ebenfalls zur Einhaltung des Datenschutzes – mit entsprechender Haftungsfolge (siehe unten) – zu verpflichten. Während nach dem BDSG noch ausschließlich der Auftraggeber als „Herr der Daten" alleine für die Datenverarbeitung und damit für die Einhaltung eines ausreichenden Datenschutzstandards verantwortlich war, finden sich in der DSGVO zahlreiche Verpflichtungen, die sich auch an den Auftragsverarbeiter richten. Diese Verpflichtungen sind in die bisherigen Verträge zur Auftragsdatenverarbeitung zu integrieren, um diese DSGVO-konform zu gestalten. So ist nach Artikel 30 Absatz 2 DSGVO auch der Auftragsverarbeiter, der Auftragnehmer, zur Führung von Verfahrensverzeichnissen verpflichtet.

Nach Artikel 32 Absatz 1 DSGVO trifft die Pflicht zu technischen und organisatorischen Maßnahmen der Datensicherheit nicht nur den Auftraggeber, sondern auch den Auftragsverarbeiter. Nach Artikel 37 Absatz 1 DSGVO hat auch der Auftragsver-

arbeiter – sofern die weiteren gesetzlichen Voraussetzungen vorliegen – einen Datenschutzbeauftragten zu bestellen. In Konsequenz ergibt sich aus Artikel 82, dass jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Schadensersatzansprüche sowohl gegen den Auftraggeber als auch gegen den Auftragsverarbeiter, den Auftragnehmer, geltend machen kann.

Allerdings bestehen zugunsten des Auftragsverarbeiters, der auf Weisung des Auftraggebers handelt und für den nur einige Verpflichtungen nach der DSGVO greifen, Entlastungs-Tatbestände, die sich in Artikel 82 Absatz 2 DSGVO wiederfinden. So haftet ein Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er einer speziell den Auftragsverarbeitern auferlegte Pflicht aus der DSGVO nicht nachgekommen ist oder wenn er ihm rechtmäßig erteilte Weisungen des Auftraggebers missachtet hat. Nach Artikel 82 Absatz 3 DSGVO ist ihm ebenfalls der Nachweis gestattet, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Begleitet wird dieser Schadensersatzanspruch der betroffenen Person auch durch Bußgelder, die wiederrum die Datenschutzbehörden nach den Artikeln 83 Absatz 3 und Absatz 4 a) DSGVO gegen den Auftragsverarbeiter verhängen können.

Rechenschaftspflicht

Das datenverarbeitende Unternehmen ist schließlich für die Einhaltung der Vorgaben der DSGVO verantwortlich und muss die Einhaltung aller zuvor genannten Datenschutz-Prinzipien nachweisen können. Dazu ist eine entsprechende Dokumentation notwendig, deren Umfang aber von der Größe des Unternehmens beziehungsweise der Menge und der Qualität der personenbezogenen Daten abhängig gemacht werden kann.

Um sich einen Überblick über die eigenen Datenverarbeitungstätigkeiten zu verschaffen, sollten Unternehmen zunächst eine Bestandsaufnahme über die Vorgänge und Prozesse machen, bei denen personenbezogene Daten erhoben, gespeichert und verarbeitet werden (nachfolgend Verarbeitungstätigkeiten). Diese Bestandsaufnahme dient im weiteren Verlauf als wichtiger Schritt, um den Umsetzungsbedarf zu analysieren. Zunächst sollte also ermittelt und festgehalten werden, im Rahmen welcher Vorgänge und Prozesse solche personenbezogenen Daten erhoben, gespeichert und verarbeitet werden. Typische Verarbeitungstätigkeiten sind etwa:

- Webseite
- Onlineshop
- Kunden-Datenverarbeitung
- Personal-Management
- Bewerber-Management
- Video-Überwachung

Im Rahmen der Bestandsaufnahme sollte jeder Verarbeitungsvorgang zunächst mit einer allgemeinen Beschreibung, Informationen über Art und Zweck der Verarbeitung, Informationen über die verarbeiteten Daten-Kategorien (wie Beschäftigtendaten) und einer Übersicht der betroffenen Personen (etwa die Mitarbeiter) schriftlich zusammengefasst werden.

In der Regel werden die wesentlichen Datenverarbeitungsvorgänge mit einem Verarbeitungsverzeichnis erfasst, in dem auch die Erfüllung der weiteren datenschutzrechtlichen Anforderungen (etwa Legitimations-Tatbestand, Erfüllung der Informationspflichten) abgeprüft und dokumentiert werden können.

Zehn Punkte zur Umsetzung der EU-DSGVO

Mit dem nachfolgenden Maßnahmenplan werden die wesentlichen Neuregelungen der Datenschutz-Grundverordnung umgesetzt.

01 „Organisatorische Maßnahmen“

Unternehmen sollten prüfen, ob sie organisatorisch hinreichend für die DSGVO aufgestellt sind. Soweit nicht bereits ein Datenschutzbeauftragter bestellt ist, sollte geprüft werden, ob eine Bestellung nicht zwingend ist. Eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht in folgenden Fällen:

- Wenn zumindest zehn Mitarbeiter regelmäßig mit automatisierter Datenverarbeitung (Erhebung und Nutzung) zu tun haben
- Wenn personenbezogene Daten verarbeitet werden, die über Rasse, ethnische Herkunft, politische Meinung, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben einer Person informieren
- Wenn personenbezogene Daten geschäftsmäßig übermittelt, erhoben, verarbeitet oder genutzt werden

Zudem sollten Geschäftsleitung und Mitarbeiter rechtzeitig über die konkreten Folgen der DSGVO und die konkreten Maßnahmen zur Umstellung informiert werden.

02 „Bestandsaufnahme durchführen“

Unternehmen sollten zunächst die beschriebene Bestandsaufnahme bezüglich aller Vorgänge und Prozesse (nachfolgende Verarbeitungstätigkeiten) durchführen, bei denen personenbezogene Daten erhoben, verarbeitet oder weitergegeben werden. Auf Grundlage der Bestandsaufnahme sollte der konkrete Änderungsbedarf identifiziert werden.

03 „Rechtsgrundlagen prüfen“

Es ist zu prüfen, ob die identifizierten Datenverarbeitungsprozesse den Anforderungen der DSGVO, insbesondere den Rechtmäßigkeitsanforderungen des Artikels 6 DSGVO, entsprechen. Ansonsten sind die Prozesse den neuen Anforderungen anzupassen.

04 „Informationspflichten erfüllen“

Die weitreichenden Informationspflichten (Artikel 13 und 14 DSGVO), die teilweise neue Anforderungen enthalten (wie Nennung der Legitimations-Grundlage, Information über Beschwerde-Recht bei Aufsichtsbehörde), sind in den internen Dokumenten (wie Kundenverträgen) und Prozessen umzusetzen.

05 „Datenschutz- und Einwilligungserklärungen umstellen“

Etwaige Datenschutz-Erklärungen (etwa auf der Webseite) oder Einwilligungserklärungen (wie für die Zusendung von E-Mail-Werbung) sind mit Hinblick auf die neuen Anforderungen (insbesondere die Informationspflichten aus Artikel 13 DSGVO) anzupassen.

06 „(Verträge über) Datenweitergabe checken“

Unternehmen sollten bei der Weitergabe von personenbezogenen Daten prüfen, auf welcher Rechtsgrundlage diese Weitergabe erfolgt. In Fällen einer Weitergabe oder Offenlegung personenbezogener Daten an Dritte zur Verarbeitung im Auftrag des Unternehmens sollten Vereinbarungen über eine Auftragsverarbeitung im Sinne des Artikels 28 DGSVO geschlossen beziehungsweise bestehende Verträge zur Auftrags(-daten-)verarbeitung überprüft und nötigenfalls überarbeitet werden.

07 „Datensicherheit umsetzen“

Die Anforderungen, die die DSGVO (etwa bezüglich Software) schon bei der Technikgestaltung und zu den Voreinstellungen (Artikel 25 DSGVO) stellt, sind umzusetzen.

08 „Datenschutzfolgen-Abschätzung durchführen“

Unternehmen haben im Rahmen einer Datenschutzfolgen-Abschätzung (Artikel 35 DSGVO) zu prüfen, ob die eigenen Datenverarbeitungsvorgänge aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Das Ergebnis und etwaige Maßnahmen zur Reduzierung eines möglichen Risikos sind zu dokumentieren.

09 „Betroffenenrechte umsetzen“

Die in der DSGVO geregelten Betroffenenrechte (wie Recht auf Auskunft oder Recht auf Löschung) müssen in den unternehmensinternen Abläufen so abgebildet sein, dass diese gegenüber den Betroffenen umgesetzt werden können.

10 „Dokumentation organisieren“

Aufgrund der vermehrten Dokumentationspflichten der DSGVO (wie Artikel 30, 33 Absatz 5, 28 Absatz 3 lit. a) DSGVO) sollte das Unternehmen die notwendige Dokumentation (etwa in Form eines Verarbeitungsverzeichnisses) organisieren.

Die weiteren Anforderungen der e-Privacy-Verordnung

Die e-Privacy-Verordnung, deren Auswirkungen bereits intensiv diskutiert werden, liegt derzeit nur im Entwurf vor. Dieser sieht einige weitreichende Änderungen bezüglich der Verarbeitung elektronischer Kommunikationsdaten, der Speicherung von Informationen in Endeinrichtungen (wie Cookies), aber auch im Bereich des Direkt-Marketings vor.

Derzeit ist noch unklar, inwieweit an dem Verordnungstext noch Änderungen vorgenommen werden beziehungsweise wann die e-Privacy-Verordnung wirksam werden soll. Aufgrund politischer Diskussionen und der Notwendigkeit weiterer Abstimmungen im Rahmen des Gesetzgebungsverfahrens ist nach den aktuellen Informationen davon auszugehen, dass die e-Privacy-Verordnung nicht vor dem Jahr 2019 Wirkung entfalten wird.

Dr. Carsten Ulbricht
carsten.ulbricht@bartsch.law

Critical Patch Update April 2018

Oracles neuestes Critical Patch Update schließt 251 Sicherheitslücken bei Hunderten von Oracle-Lösungen. Einige der angesprochenen Sicherheitslücken betreffen mehrere Produkte. Die meisten Sicherheitslücken liegen bei Fusion Middleware (40), Oracle Financial Services Applications (36), MySQL (33) und Retail Applications (31). Aufgrund der Bedrohung durch einen erfolgreichen Angriff empfiehlt Oracle seinen Kunden dringend, die Critical Patch Update Fixes so schnell wie möglich anzuwenden. Eine komplette Liste der betroffenen Produkte ist auf der Website *„http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html“* abrufbar. Oracle veröffentlicht alle drei Monate ein Critical Patch Update. Die nächsten Termine sind 17. Juli 2018, 16. Oktober 2018 und 15. Januar 2019.