Die Herausforderung des Jahres: Die Datenschutz-Grundverordnung

Dr. Anke Reich L.L.M

Gerade in den letzten Monaten hat der Datenschutz durch die Datenschutz-Grundverordnung (DSGVO) viel von sich Reden gemacht. Diese gilt seit dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten der Europäischen Union und bringt teils weitreichende Änderungen gegenüber der bisherigen Rechtslage mit sich.

Betroffen sind alle Unternehmensbereiche, in denen personenbezogene Daten erhoben, gespeichert oder in anderer Weise verarbeitet werden – und zwar unabhängig davon, ob dies auf elektronischem Wege oder durch automatisierte Verfahren erfolgt oder nicht. Der praktische Anwendungsbereich ist somit viel umfassender als oftmals gedacht wird. Insbesondere wegen des im Vergleich zur derzeitigen Rechtslage vielfach höheren Bußgeldrisikos bei Datenschutzverstößen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes sollte dem Thema die gebotene Aufmerksamkeit geschenkt werden.

Anwendungsbereich der DSGVO

Die DSGVO „enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten." (Art. 1 Abs. 1 DSGVO). Mit anderen Worten: Die DSGVO ist zu beachten, sobald und solange personenbezogene Daten verarbeitet werden.

a) Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen" (Art. 4 Nr. 1 DSGVO). Dies sind insbesondere Vorname, Nachname, Adresse, Telefonnummer, Telefaxnummer, E-Mail-Adresse, Geburtsdatum und Bankverbindung, aber auch Daten über Nutzung von Telefon und (nach umstrittener Ansicht) auch IP-Adressen, wenn diese bei der Nutzung von Internetseiten gespeichert werden. Zu beachten ist zudem, dass bei besonderen Kategorien personenbezogener Daten (vgl. Art. 9 und 10 DSGVO, z. B. solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen) besonders strenge Datenschutzbestimmungen gelten.

b) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter „Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung." (Art. 4 Nr. 2 DSGVO).

Im Unternehmeralltag finden vielfältige Verarbeitungsprozesse statt. So werden beispielsweise personenbezogene Daten von Kunden, Lieferanten und Mitarbeitern erhoben und oftmals in Datenbanken gespeichert. Möglicherweise werden auch personenbezogene Daten durch ein Kontaktformular im Internetauftritt des Unternehmens erfragt. Falls auf der Internetseite eines Unternehmens Cookies eingesetzt werden, die die IP-Adresse speichern und damit das Nutzerverhalten erkennbar machen, muss dies ebenfalls datenschutzkonform ausgestaltet sein.

Zu beachten ist zudem, dass wenn die personenbezogenen Daten nicht in Datenbanken gespeichert werden, sondern manuell ohne technische Hilfsmittel, die DSGVO ebenfalls eingehalten werden muss, wenn die Daten in einem Dateisystem (= jede strukturierte Sammlung von Informationen, die nach bestimmten Kriterien geordnet sind) gespeichert werden.

Wichtige Punkte hinsichtlich der Verarbeitung personenbezogener Daten

Nachfolgend seien aus der Fülle der durch die DSGVO auferlegten und von jedem Unternehmen zu beachtenden Anforderungen einige Wichtige hervorgehoben:

a) Erstellung oder Aktualisierung eines Verzeichnisses von Verarbeitungstätigkeiten

Nach Art. 30 DSGVO besteht regelmäßig eine Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten, es sei denn, bei einem Unternehmen sind weniger als 250 Mitarbeiter beschäftigt, es besteht kein Risiko für die Rechte und Freiheiten der Betroffenen, die Verarbeitung erfolgt nicht nur gelegentlich und es sind keine besonderen Kategorien (Art. 9, 10 DSGVO) betroffen. Da die Verarbeitung von personenbezogenen Daten bei vielen Unternehmen nicht nur gelegentlich erfolgt, werden wohl die allermeisten Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten führen müssen. Dies muss schriftlich oder elektronisch erfolgen.

„Jeder Verantwortliche muss dafür Sorge tragen, dass ein Verzeichnis von Verarbeitungstätigkeiten vorhanden ist."

Das Verzeichnis von Verarbeitungstätigkeiten gibt eine Übersicht über alle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden. Durch diese Pflicht wird die allgemeine Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) konkretisiert.

b) Einwilligungen

Da jede Verarbeitungstätigkeit nur rechtmäßig ist, wenn entweder ein gesetzlicher Erlaubnistatbestand

Wichtige Angaben laut DSVGO

Nach Art. 30 Abs. 1 DSGVO muss das Verzeichnis von Verarbeitungstätigkeiten insbesondere folgende Angaben enthalten:

- Name und Kontaktdaten des Verantwortlichen
- Name und Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien von Empfängern
- ggf. Übermittlung personenbezogener Daten an ein Drittland

Das Verzeichnis von Verarbeitungstätigkeiten muss Kunden und Mitarbeitern nicht zugänglich sein, aber der Aufsichtsbehörde auf Verlangen vorgelegt werden können. Andernfalls droht ein Bußgeld bis zu 20 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes (Art. 83 Abs. 4 a) i.V.m. Art. 30 Abs. 4 DSGVO).

eingreift oder eine Einwilligung vorliegt, muss in jedem Fall, in dem die Datenverarbeitung nicht durch das Gesetz erlaubt ist, eine Einwilligung nach den Anforderungen des Art. 6, 7 DSGVO vorliegen.

Bei Einwilligungserklärungen in Allgemeinen Geschäftsbedingungen gelten darüber hinaus besondere Anforderungen.

ACHTUNG: Bei Verstoß gegen datenschutzrechtliche Anforderungen bei der Einwilligung greift die höchste Bußgeldkategorie (Art. 83 Abs. 5 DSGVO) ein, d.h. es drohen Geldbußen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes.

c) Bestellung eines Datenschutzbeauftragten

Nach Art. 37 DSGVO ergibt sich eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten für Unternehmen, deren Kerntätigkeit entweder eine „umfangreiche regelmäßige und systematische Beobachtung" Betroffener erfordert oder aus einer umfangreichen Verarbeitung besonderer Kategorien von Daten besteht. Art. 37 Abs. 4 S. 1 HS 2 DSGVO erlaubt den Mitgliedstaaten jedoch, die Pflicht zur Bestellung auszuweiten. Davon hat der deutsche Gesetzgeber Gebrauch gemacht und in § 38 Abs. 1 BDSG bestimmt, dass eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht,

- soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung beschäftigt sind

oder

- unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, wenn Verarbeitungen durchgeführt werden, die der Datenschutz-Folgenabschätzung unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

ACHTUNG: Wenn eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, ist ein Datenschutzbeauftragter zu benennen.

Angesichts der Aufgabe des Datenschutzbeauftragten, für Betroffene als Ansprechpartner zur Verfügung zu stehen (Art. 38 Abs. 4 DSGVO), sollten die Kontaktdaten jederzeit abrufbar sein, z.B. im Intra- oder Internet. Bei einem Verstoß gegen diese Vorschrift ist ein Bußgeld bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes möglich (Art. 83 Abs. 4 a) DSGVO).

d) Prüfung und ggf. Abschluss von Verträgen

aa) Vertrag mit Auftragsverarbeiter

Wenn personenbezogene Daten auf Weisung des Verantwortlichen durch Dritte verarbeitet werden, liegt eine Auftragsverarbeitung vor. Dies ist beispielsweise der Fall, wenn personenbezogene Daten von Kunden im Internet erhoben werden und die Daten auf den Servern des Anbieters liegen.

Als Mindestinhalt sind die in Art. 28 Abs. 3 DSGVO aufgelisteten Punkte aufzunehmen. Jedem Unternehmen ist anzuraten, zu prüfen, ob und welche Dienstleister zur Verarbeitung personenbezogener Daten eingesetzt werden und in welcher Weise eine Datenverarbeitung stattfindet.

„Mit solchen Dienstleistern – die gleichsam als langer Arm des Verantwortlichen agieren – müssen Verträge über die Auftragsverarbeitung bestehen bzw. geschlossen werden."

bb) Vertrag wegen gemeinsamer Verantwortlichkeit

Wenn zwei Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen, liegt eine sog. gemeinsame Verantwortung vor (Art. 26 DSGVO) und es sind besondere Anforderungen einzuhalten.

e) Wahrung der Betroffenenrechte

Betroffene (v. a. Kunden, Lieferanten und Mitarbeiter) haben insbesondere folgende Rechte:

- Informationsrechte, Art. 12, 13, 14 DSGVO
- Auskunftsrecht, Art. 12, 15 DSGVO
- Recht auf Berichtigung, Art. 12, 16 DSGVO
- Recht auf Löschung von personenbezogenen Daten, deren Zweck erfüllt ist und bei denen keine gesetzliche Aufbewahrungspflicht besteht (sog. Recht auf Vergessenwerden), Art. 12, 17 DSGVO
- Recht auf Einschränkung der Verarbeitung, Art. 12, 18 DSGVO
- Recht auf Datenübertragbarkeit, Art. 12, 20 DSGVO
- Widerspruchsrecht, Art. 12, 21 DSGVO

Bestehende Mitteilungen, Erklärungen (einschließlich Datenschutzerklärung auf der Internetseite) sollten überprüft und ggf. aktualisiert werden. Wenn festgestellt werden sollte, dass betroffenen

Personen, bei denen bereits Daten erhoben worden sind, beispielsweise nicht alle erforderlichen Informationen zur Verfügung gestellt worden sind, musste dies bis zum 25. Mai 2018 nachgeholt werden, um datenschutzkonform zu handeln.

ACHTUNG: Bei einem Verstoß gegen datenschutzrechtliche Anforderungen bei den Betroffenenrechten greift die höchste Bußgeldkategorie von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes (Art. 83 Abs. 5 DSGVO) ein.

f) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nach Art. 24 Abs. 1 DSGVO besteht die allgemeine Pflicht des Verantwortlichen, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass Datenschutzkonformität eingehalten und nachgewiesen werden kann.

Konkretisierend verpflichtet Art. 25 Abs. 1 DSGVO zum Datenschutz durch Technikgestaltung und Art. 25 Abs. 2 DSGVO zu datenschutzfreundlichen Voreinstellungen (d.h. durch Voreinstellungen dürfen nur Daten erhoben und nur so lange gehalten werden, wie sie nach dem Zweck erforderlich sind).

Bei allen Datenverarbeitungsvorgängen sollte insbesondere geprüft werden, ob ausreichende Sicherheitsvorkehrungen getroffen worden sind (Datensicherung, Verschlüsselung, etc.) und beispielsweise alle anzugebenden Pflichtangaben in Formularen tatsächlich erforderlich sind.

g) ggf. Datenschutz-Folgeabschätzung

Nach der Art der Datenerhebung kann eine Datenschutz-Folgeabschätzung erforderlich sein, Art. 35 DSGVO. Dies ist der Fall, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten zur Folge hat, z. B. wenn besondere Kategorien von personenbezogenen Daten verarbeitet werden. Die Mindestinhalte dieser Folgeabschätzung ist in Art. 35 Abs. 7 DSGVO festgeschrieben. Vor Beginn der Verarbeitung ist nach Art. 36 DSGVO die Aufsichtsbehörde zu konsultieren.

„Alle Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (Art. 12 Abs. 1 DSGVO).“

h) Meldepflichten bei Verstößen

Eine Datenschutzverletzung ist innerhalb von 72 Stunden der Aufsichtsbehörde zu melden, nachdem die Verletzung bekannt geworden ist (Art. 33 DSGVO).

Damit dieser Zeitraum in jedem Einzelfall gewahrt werden kann, sollte vorab festgelegt werden, wer wann welche Informationen an die Aufsichtsbehörde meldet. Der Mindestinhalt einer solchen Meldung ist in Art. 33 Abs. 3 DSGVO geregelt.

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folgte hat, ist zudem die betroffene Person unverzüglich zu benachrichtigen (Art. 34 DSGVO). Bei einem Verstoß gegen diese Meldepflichten droht jeweils ein Bußgeld bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes (Art. 83 Abs. 4 a) DSGVO)

i) Richtlinie für Umsetzung des Datenschutzes

Bestenfalls sollte in einer Richtlinie ein Datenschutzmanagement implementiert werden, damit innerhalb eines Unternehmens jede Person weiß, wer für bestimmte Fragen des Datenschutzes zuständig ist und handelt. Es sollte insbesondere ein Konzept für die Löschung der Daten und wie bei Datenpannen zu verfahren ist, erarbeitet werden, um die Vorgaben der DSGVO einzuhalten. [5330]

Fazit – Jeder ist selbst für sein Unternehmen verantwortlich

Die DSGVO bringt teils weitreichende Änderungen mit sich. Jeder Verantwortliche ist für sein eigenes Unternehmen verantwortlich und muss selbständig dafür Rechnung tragen, dass sämtliche Datenschutzrechtliche Anforderungen eingehalten werden. Daran ändert auch die Bestellung eines Datenschutzbeauftragten nichts.

Nicht zuletzt wegen der teils sehr hohen Bußgelder bei Datenschutzverstößen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes ist es jedem Unternehmen im ganz eigenen Interesse anzuraten, bestenfalls sämtliche Vorgänge in denen personenbezogene Daten erhoben, gespeichert, gelöscht oder sonst verarbeitet werden, gründlich auf deren Rechtmäßigkeit nach der DSGVO zu überprüfen und ggf. externe Hilfe in Anspruch zu nehmen. Dabei bringt die DSGVO nicht nur Pflichten und Risiken mit sich, sondern bietet gleichzeitig die Möglichkeit, sich von der Konkurrenz positiv abzuheben. Ein gutes Datenschutz-Management-System kann im Vergleich zu Mitbewerbern daher ein entscheidender Wettbewerbsvorteil sein.