ComplianceBusiness
Ausgabe 2 // Juni 2016

EU-Datenschutzgrundverordnung – bleibt alles anders?!

Von Dr. Jan-Peter Ohrtmann und Matthias Bleidiesel

Einführung

Nachdem die EU-Datenschutzgrundverordnung (DS-GVO) am 25.05.2016 in Kraft getreten ist, müssen Unternehmen nun die Vorgaben in den nächsten zwei Jahren bis zum 25.05.2018 umsetzen. Dabei gilt: Vieles bleibt gleich, manches wird anders, einiges kommt neu hinzu. Eine Auseinandersetzung mit dem Thema Datenschutz ist nun unvermeidlich, insbesondere für diejenigen Unternehmen, bei denen der Datenschutz wenig belastbar implementiert ist. Denn bei Verstößen drohen massiv erhöhte Bußgelder von bis zu 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes – pro Verstoß, versteht sich.

Vor diesem Hintergrund stellen sich die Fragen, was noch erlaubt ist und an welcher Stelle die bestehenden Prozesse verändert werden müssen. Dazu werden die Datenverarbeitungsprozesse, die Organisation, die bereits verwendeten Einwilligungserklärungen und Verträge auf den Prüfstand einer Gap-Analyse gestellt werden müssen. Im Einzelnen:

Was ist noch erlaubt? – Erlaubnistatbestände

Ein Blick in die Erlaubnistatbestände der DS-GVO in Art. 6 bis 10 zeigt viel Bekanntes, aber auch viele Änderungen. Das datenschutzrechtliche Prinzip des Verbots mit Erlaubnisvorbehalt liegt auch der DS-GVO zugrunde, wonach die Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten ist, sofern die Verarbeitung nicht ausdrücklich gesetzlich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat. Eine wesentliche Herausforderung für die Unternehmen wird in den nächsten zwei Jahren die Klärung der Frage sein, auf welcher Rechtsgrundlage die Verarbeitung personenbezogener Daten im Unternehmen erfolgen darf:

Einwilligung

Auf den ersten Blick sind die Voraussetzungen für eine Einwilligung nicht wesentlich verändert worden. Art. 7 DS-GVO, der die Voraussetzungen einer Einwilligung im Sinne des Art. 6 Abs. 1 lit. a) DS-GVO regelt, beinhaltet eine ähnliche Struktur wie das bestehende Recht. Dennoch dürfte die datenschutzrechtliche Einwilligung ▸

Der Schutz von persönlichen Daten ist nicht nur eine strafbewehrte Pflicht. Verstöße können die Reputation empfindlich schädigen.

zu den Feldern gehören, die den Unternehmen bei der Umsetzung der DS-GVO einen erheblichen Umsetzungsaufwand abverlangen werden. Denn angesichts der gestiegenen Transparenzanforderungen nach Art. 13 DS-GVO ist davon auszugehen, dass dem Betroffenen für eine wirksame informierte Einwilligung deutlich mehr Informationen zur Verfügung gestellt werden müssen als bislang.

Für die Unternehmen ergibt sich aus den veränderten Anforderungen der DS-GVO zunächst die Notwendigkeit, die bestehenden Einwilligungserklärungen und Formulare für Einwilligungserklärungen dahingehend zu prüfen, ob sie nach dem 25.05.2018 noch wirksam sind. Nach Erwägungsgrund 173 der DS-GVO genießen bestehende Einwilligungserklärungen keinen Bestandsschutz, sondern müssen ab dem 25.05.2018 den Anforderungen der DS-GVO entsprechen. Tun sie dies nicht, müssen sie neu eingeholt werden.

Gesetzliche Erlaubnistatbestände

Ein auffälliger Kontrast zum Bundesdatenschutzgesetz (BDSG) ist, dass die vom deutschen Gesetzgeber zum Teil sehr detaillierten und ausdifferenzierten Erlaubnistatbestände, namentlich in §§ 28, 29 BDSG, in dieser Detaillierung in der DS-GVO nicht enthalten sind. Viele der expliziten Erlaubnistatbestände für bestimmte Verarbeitungssituationen, wie etwa die Datenübermittlung an Auskunfteien (§ 28a BDSG), sowie die Regelung zur Datenerhebung zur Markt- und Meinungsforschung (§ 30a BDSG) sind nicht mehr in der DS-GVO enthalten. Mehr noch als heute ergibt sich die Zulässigkeit vielmehr aus einer Interessenabwägung. Dies birgt Chancen bei der Gestaltung der Prozesse und der rechtlichen Argumentation, aber auch Rechtsunsicherheiten. Auf der Suche nach Anwendungsfällen hilft dabei teilweise ein Blick in die Erwägungsgründe, die beispielhaft Verarbeitungssituationen benennen, die in den Anwendungsbereich der jeweiligen Erlaubnisnorm fallen können.

Datenverarbeitung für eigene Geschäftszwecke

Die Verarbeitung zum Zweck der Erfüllung eines Vertragsverhältnisses und zur Erfüllung einer gesetzlichen Pflicht findet sich in Zukunft in Art. 6 Abs. 1 lit b) und c) DS-GVO. Sie ist stark an das aktuelle Recht angelehnt. Art. 6 Abs. 1 lit. f) DS-GVO beinhaltet den Erlaubnistatbestand der Verarbeitung zur Wahrung überwiegender berechtigter Interessen. Insbesondere Marketing und Werbung sowie sonstige CRM-Maßnahmen werden in Zukunft auf diese Norm gestützt werden müssen. Da weder Listenprivileg noch Adresshandel, die zurzeit in § 28 Abs. 3 BDSG eine Regelung finden, in der DS-GVO ausdrücklich geregelt sind, wird im Einzelfall zu bewerten sein, ob überwiegende berechtigte Interessen die Verarbeitung rechtfertigen oder eine Einwilligung der Betroffenen erforderlich sein wird.

Konzerninterner Datentransfer

Da das aktuelle Datenschutzrecht kein Konzernprivileg kennt, muss jeder konzerninterne Transfer von personenbezogenen Daten wie ein Datentransfer zu Dritten datenschutzrechtlich gerechtfertigt werden. Zwar enthält auch die DS-GVO kein explizites Konzernprivileg. Allerdings findet sich in Erwägungsgrund 48 die Aussage, dass Verantwortliche ein berechtigtes Interesse haben können, „personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln“. Dies indiziert, dass der Weitergabe zu diesen Zwecken im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f) ein substantielles Interesse zuzumessen und die Weitergabe möglicherweise einfacher zu rechtfertigen ist als bislang.

Beschäftigtendaten

Die DS-GVO enthält keine spezifischen Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten. Insbesondere fehlt es an einer dem § 32 BDSG entsprechenden Regelung. Die allgemeinen Erlaubnistatbestände der DS-GVO haben auch im Beschäftigungsverhältnis Geltung. Je nach Verarbeitungssituation kommen unterschiedliche Rechtsgrundlagen in Betracht. Die für die Erfüllung des Arbeitsvertrags erforderlichen Verarbeitungsvorgänge erfolgen auf Basis von Art. 6 Abs. 1 lit. b) DS-GVO (Verarbeitung erforderlich für die Erfüllung eines Vertragsverhältnisses). Die Verarbeitung von Gesundheitsdaten im Beschäftigungsverhältnis richtet sich nach den Regeln des Art. 9 DS-GVO, der die Verarbeitung von sensitiven Daten regelt. Für weitere Verarbeitungen, beispielsweise Compliancekontrollen, Fraud-Control- ▸

ComplianceBusiness
Ausgabe 2 // Juni 2016

Maßnahmen oder sonstige Überwachungsmaßnahmen kommt als Rechtsgrundlage die Wahrung berechtigter Interessen in Betracht [Art. 6 Abs. 1 lit f) DS-GVO].

Ob es dabei bleibt, ist noch ungewiss. Die DS-GVO räumt in Art. 88 den nationalen Gesetzgebern die Möglichkeit ein, durch Rechtsvorschrift oder Kollektivvereinbarung spezielle Vorschriften für den Datenschutz im Beschäftigungsverhältnis zu erlassen. Ob der deutsche Gesetzgeber von dieser Öffnungsklausel Gebrauch macht und einen neuen Anlauf unternimmt, sein umstrittenes Projekt zum Beschäftigtendatenschutz weiterzuverfolgen, ist noch ungewiss. Wie sich der Beschäftigtendatenschutz unter der DS-GVO weiterentwickeln wird, bleibt also abzuwarten. Weiterhin kann auch eine Betriebsvereinbarung die Datenverarbeitung rechtfertigen.

Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung (Art. 28 DS-GVO) bleibt weiterhin möglich. Sie orientiert sich auch weitgehend an der Systematik des § 11 BDSG. Eine Anpassung der Verträge zur Auftragsdatenverarbeitung wird daher vor allem für die Konzerngesellschaften erforderlich sein, die nicht deutschem Datenschutzrecht – in der Regel dem BDSG – unterliegen und dementsprechend nach nationalem Recht „schlankere" Verträge abgeschlossen haben. Unter Umständen wird die EU-Kommission gemäß Art. 28 Abs. 6 DS-GVO von der Möglichkeit Gebrauch machen, einen Mustervertrag für die Auftragsdatenverarbeitung bereitzustellen.

Die Einhaltung der Verpflichtungen des Auftragnehmers zu den technischen und organisatorischen Maßnahmen kann nun gemäß Art. 28 Abs. 5 DS-GVO durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens nach Art. 42 DS-GVO nachgewiesen werden. Daneben entfällt die im BDSG explizit geforderte laufende Prüfungspflicht durch den Auftraggeber.

Drittlandtransfer

Beim Drittlandtransfer sind ebenso keine wesentlichen Veränderungen zu verzeichnen. Ein Angemessenheitsbeschluss der EU-Kommission ist weiterhin ausreichend (Art. 45 DS-GVO), wie der Nachweis „geeigneter Garantien" (Art. 46 DS-GVO), um Daten an einen Dienstleister in einem Drittland übermitteln zu dürfen. Mögliche Garantien sind beispielsweise verbindliche interne Datenschutzvorschriften (sogenannte Binding Corporate Rules), genehmigte Verhaltensregeln (sogenannter Code of Conduct) oder Standardvertragsklauseln. Ob und inwieweit die EU-Standardvertragsklauseln eine Übermittlung in Drittländer weiterhin ermöglichen, liegt dem Europäischen Gerichtshof derzeit zur Entscheidung vor.

Transparenz

Die meisten in der DS-GVO vorgesehenen Betroffenenrechte sind vom Grundsatz her aus dem BDSG bekannt. Erheblich gestärkt wurden allerdings der Transparenzgrundsatz und damit die Informationspflichten gegenüber den Betroffenen. Nach Art. 13 DS-GVO sind den Betroffenen bei Datenerhebung deutlich umfassendere Informationen mitzuteilen. Damit dürften faktisch alle Datenschutzerklärungen und Privacy-Policies überarbeitet werden müssen.

Betroffenenrechte

Zwei Neuerungen bei den Betroffenenrechten werfen in besonderem Maße praktische Fragen auf: das Recht auf Vergessenwerden und das sogenannte Recht auf Datenübertragbarkeit. Denn beide Rechte sind unscharf formuliert, und es besteht das erhöhte Risiko, dass die rechtskonforme Umsetzung durch die Geltendmachung seitens der Betroffenen auch praktisch getestet wird.

Das bislang auch schon bekannte Recht auf Löschung von Daten, wenn diese nicht mehr für den konkreten Verarbeitungszweck benötigt werden, wurde in Art. 17 DS-GVO erweitert zu einem „Recht auf Vergessenwerden". Hierzu regelt Abs. 2, dass ein Verantwortlicher, der die Daten öffentlich gemacht hat und zu einer Löschung verpflichtet ist, angemessene Maßnahmen treffen muss, um die Datenempfänger ebenfalls über das Löschbegehren des Betroffenen zu informieren. Wie weitgehend diese Pflicht ist, geht nicht klar aus Art. 17 DS-GVO hervor. Jedenfalls müssen Unternehmen mehr denn je die Datenflüsse kennen und unter Kontrolle halten.

Das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) ist ein datenschutzrechtliches Novum. Demnach hat

ComplianceBusiness
Ausgabe 2 // Juni 2016

der Betroffene das Recht, die ihn betreffenden personenbezogenen Daten, die er für einen Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Data Protection Impact Assessment (DPIA)

Die Datenschutz-Folgenabschätzung (Data Protection Impact Assessment) nach Art. 35 DS-GVO ist neu eingefügt worden, wenngleich der Gedanke der Vorabkontrolle nach § 4d Abs. 5 BDSG nicht unbekannt ist. Der Anwendungsbereich der Datenschutz-Folgenabschätzung ist erweitert worden, weil künftig auch alle Verarbeitungen mit einem voraussichtlich hohen Risiko für Freiheitsrechte einer Prüfung unterzogen werden müssen.

Data Protection by Default/Data Protection by Design

Die gewachsene Bedeutung des Datenschutzes für die Geschäftsprozesse von Unternehmen zeigt sich auch in den eingeführten Grundsätzen Data Protection by Default und Data Protection by Design. Gemäß Art. 25 DS-GVO müssen diese Grundsätze schon beim Produkt- und Servicedesign berücksichtigt werden. Damit wird die Datenschutzcompliance mehr denn je auch ein Thema für den Produktionsprozess.

Datenschutzbeauftragter

Die Rolle des Datenschutzbeauftragten wird EU-weit eingeführt, Art. 37 bis 39 DS-GVO. Ein Datenschutzbeauftragter ist nach Art. 37 Abs. 1 lit b) und c) DS-GVO zu bestellen, sofern die Kerntätigkeit des Unternehmens in Verarbeitungsvorgängen besteht, die eine Überwachung von Personen erfordert, oder sofern die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Arten personenbezogener Daten liegt. Dies bringt eine gewisse Unschärfe mit sich. Allerdings könnte Deutschland von der Möglichkeit nach Art. 37 Abs. 4 DS-GVO Gebrauch machen und eine nationale Regelung zur verpflichtenden Bestellung eines Datenschutzbeauftragten schaffen. Dann hätten deutsche Unternehmen den doppelten Aufwand: Sie müssten den Datenschutzbeauftragten bestellen, wären aber nicht mehr von der Meldepflicht der Datenverarbeitung gegenüber der Aufsicht (Konsultation nach Art. 36 DS-GVO) befreit, wie dies noch im BDSG grundsätzlich der Fall ist.

Fazit

Unternehmen sollten die scheinbar lange Übergangsphase nicht unterschätzen und die Transformation zur DS-GVO beginnen, um das Risiko von hohen Bußgeldern von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes ab Mai 2018 zu reduzieren. Zur Projektplanung empfehlen sich zunächst eine Reevaluierung der Datenschutzstrategie (Welche Bedeutung hat der Datenschutz für das Unternehmen angesichts des geänderten Risikoprofils?) und eine Festlegung der Umsetzungsbreite und -tiefe (In welchen Risikobereichen soll welcher Reifegrad erreicht werden?). Danach sollten die relevanten Prozesse identifiziert und priorisiert werden. Anschließend sind die Prozesse nach künftigem Recht zu bewerten und gegebenenfalls anzupassen. Der Anpassungsbedarf des Ist/Soll-Vergleichs und damit die Implementierung betreffen dabei unterschiedliche Ebenen (rechtlich, organisatorisch, prozessual, technisch).

Dr. Jan-Peter Ohrtmann,
Rechtsanwalt, Director, PwC Legal, Praxisgruppe IP, IT und Datenschutz, Düsseldorf
jan-peter.ohrtmann@de.pwc.com
www.pwclegal.de

Matthias Bleidiesel,
Rechtsanwalt, PwC Legal, Praxisgruppe IP, IT und Datenschutz, Düsseldorf
matthias.bleidiesel@de.pwc.com
www.pwclegal.de