Luther.

IP/IT

(Intellectual Property/Information Technology)

Neue Spielregeln im Datenschutzrecht –
die EU-Datenschutzgrundverordnung und ihre Folgen

Sondernewsletter April 2016

Neue Spielregeln im Datenschutzrecht – die EU-Datenschutz-grundverordnung und ihre Folgen

Auf den Punkt.
Am 14. April 2016 hat das Europäische Parlament nach gut vier-jährigen Verhandlungen die Europäische Datenschutzgrundverordnung (DSGVO) final verabschiedet. Sie wird zukünftig die Regelungen der Europäischen Datenschutzrichtlinie 95/46/EG und die in ihrer Umsetzung erlassenen Datenschutzgesetze der EU-Mitgliedsstaaten ersetzen. Hieraus ergeben sich gravierende Neuerungen bei den maßgeblichen datenschutzrechtlichen Anforderungen an Unternehmen.

Allgemeines

a) Inkrafttreten und Übergangsfrist

Die DSGVO tritt 20 Tage nach ihrer Veröffentlichung im EU-Amtsblatt, also voraussichtlich im Mai 2016, in Kraft. Es folgt dann eine zweijährige Übergangsfrist, nach deren Ablauf im Frühjahr 2018 die DSGVO unmittelbar in allen Mitgliedstaaten der EU unmittelbare Geltung erlangt.

b) Anwendungsbereich

Der Anwendungsbereich europäischen Datenschutzrechts wird durch die DSGVO im Vergleich zu der bisherigen Rechtslage ausgedehnt. Die DSGVO gilt zwar, wie auch das bislang in der EU geltende Datenschutzrecht, für den Umgang mit personenbezogenen Daten lebender natürlicher Personen, d.h. für Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen, Art. 4 Abs. 1 DSGVO. Neben Name, Adresse, Hobbies, Standortdaten, ID-Nummern werden in Erwägungsgrund 30 der DSGVO nunmehr auch ausdrücklich IP-Adressen oder Cookies als personenbezogene Daten bezeichnet, so dass hier eine Klärung der bislang uneinheitlich bewerteten Rechtslage erfolgt ist. Identifizierbar sind nach Erwägungsgründen 26 ff. zudem ausdrücklich auch Personen, deren Daten pseudonymisiert wurden.

Die DSGVO gilt zudem ausdrücklich nur für personenbezogene Daten natürlicher Personen und nicht – wie heute von einigen deutschen Datenschutzaufsichtsbehörden vertreten – auch für solche juristischer Personen. Dies führt zu Erleichterungen im Umgang mit Daten von B2B-Kunden; allerdings ist hier zu berücksichtigen, dass auf Daten von z.B. Ansprechpartnern, die in Customer-Relationship-Management-Systemen gespeichert werden, die DSGVO sehr wohl Anwendung finden wird.

Örtlich gilt die DSGVO nach Art. 3 für alle Unternehmen mit Sitz in der EU unabhängig vom Ort der Verarbeitung. Dazu zählen die verantwortliche Stelle selbst, Auftragsdatenverarbeiter oder auch deren Niederlassungen. Zudem findet die DSGVO künftig auch Anwendung, wenn Unternehmen mit Sitz außerhalb der EU europäischen Betroffenen Waren oder Dienstleistungen (auch kostenlos) anbieten oder deren Verhalten beobachten. Erstellt daher etwa ein Anbieter mit Sitz in den USA im Internet Profile über Konsumenten für Zwecke der Absatzförderung, muss er die DSGVO beachten.

Wesentlich ist weiterhin, dass die DSGVO technologieneutral ausgestaltet ist und nicht mehr zwischen dem Online- und dem Offline-Bereich unterscheidet. Es ist daher davon auszugehen, dass z.B. die zurzeit für den Umgang mit Daten im Internet geltenden Regelungen des Telemediengesetzes entfallen werden. Bislang hat der deutsche Gesetzgeber jedoch nicht konkret Stellung genommen, auf welche Art und Weise er das nationale Recht anpassen wird, so dass es hier abzuwarten gilt.

c) Abweichende Regelungen der Mitgliedsstaaten

Die DSGVO sorgt grundsätzlich für eine Vereinheitlichung des Datenschutzrechts innerhalb der EU. Dennoch ist es den Mitgliedsstaaten unter bestimmten Voraussetzungen gestattet, abweichende bereichsspezifische Datenschutzregelungen zu erlassen. Explizit sieht dies die Verordnung beispielsweise für den Beschäftigtendatenschutz vor.

Das ändert sich im Einzelnen für Ihr Unternehmen

Auch wenn die DSGVO auf den ersten Blick den bislang in Deutschland geltenden Regelungen entspricht, ergibt sich für Unternehmen auf den zweiten Blick erheblicher Anpassungsbedarf nicht nur von Prozessen sondern auch im Umgang mit

den Daten. Die neuen Pflichten sollten ernst genommen werden, da Unternehmen umfassend haften: Nach Art. 5 Abs. 2 und 24 DSGVO gilt künftig eine erhöhte Rechenschaftspflicht (Accountability). Unternehmen müssen u.a. durch die Vorlage geeigneter Dokumente etc. nachweisen, dass der Umgang mit den Daten im Einklang mit den in der DSGVO dargestellten Grundsätzen erfolgt (siehe auch Erwägungsgrund 85). Die Rechenschaftspflicht führt zu einer Beweislastumkehr zu Lasten der verantwortlichen Stelle, so dass bereits die fehlerhafte Dokumentation der Einhaltung des Datenschutzrechts zu wirtschaftlichen Folgen für Unternehmen führen kann.

Nachfolgend ein erster Überblick:

1. Datenverarbeitung im Unternehmen: Wann und wie dürfen Daten verarbeitet werden?

Ob und unter welchen Voraussetzungen personenbezogene Daten verarbeitet und genutzt werden dürfen, ist eine der wesentlichen Stellschrauben im datenschutzrechtlichen Regelungsregime. Die DSGVO orientiert sich hier an den bereits bekannten Vorgaben: Auch künftig gilt das Verbot mit Erlaubnisvorbehalt, d.h. nur dann, wenn ein Gesetz bzw. eine Rechtsgrundlage den Umgang mit den Daten erlaubt oder die Einwilligung des Betroffenen vorliegt, ist der Umgang mit den Daten zulässig.

Neben der gesetzlichen Erlaubnis gilt – wie auch heute – die Kollektivvereinbarung bzw. Betriebsvereinbarung als Rechtsgrundlage (siehe Erwägungsgrund 155). Damit kann der Umgang mit Beschäftigtendaten auch künftig in Betriebsvereinbarungen geregelt werden.

Im Einzelnen:

a) Erlaubnistatbestände nach der DSGVO

Auf den ersten Blick haben es Unternehmen künftig leichter, da die DSGVO im Vergleich zum geltenden BDSG wesentlich weniger und mehr allgemein gefasste Erlaubnistatbestände enthält. Während das BDSG den Umgang mit Beschäftigtendaten oder auch die Nutzung von Daten für Werbezwecke, Markt- und Meinungsforschung oder auch zur Videoüberwachung in jeweils eigenen – durchaus komplizierten und widersprüchlichen - Erlaubnistatbeständen regelte, findet künftig vornehmlich Art. 6 DSGVO Anwendung. Für Unternehmen werden im Wesentlichen die folgenden Regelungen gelten:

Umgang mit Daten

- für Zwecke des Abschlusses / der Erfüllung von Verträgen oder vorvertraglichen Maßnahmen, Art. 6 Abs. 1 lit. b DSGVO;

- im Rahmen der Erfüllung rechtlicher Verpflichtungen, Art. 6 Abs. 1 lit. c DSGVO; darauf basierend darf die verantwortliche Stelle Daten z.B. nutzen, um Sozialversicherungsabgaben der Beschäftigten abzuführen oder aus steuerrechtlichen Gründen;

- im Rahmen von Interessenabwägungen; hier ist von der verantwortlichen Stelle abzuwägen, ob überwiegende berechtigte Interessen der verantwortlichen Stelle bzw. eines Dritten im Vergleich mit den schutzwürdigen Interessen, Grundrechten oder Grundfreiheiten des Betroffenen vorliegen, Art. 6 Abs. 1 lit. f DSGVO.

Daneben gelten Sondervorschriften für die Verarbeitung von besonderen personenbezogenen Daten, wie z.B. Gesundheit, Religion oder Rasse, Art. 9 DSGVO, Daten betreffend strafrechtliche Verurteilungen und Straftaten, Art. 10 DSGVO oder auch zur automatisierten Generierung von Einzelentscheidungen (inklusive Profiling), Art. 22 DSGVO. Da der nationale Gesetzgeber u.a. über den Beschäftigtendatenschutz selbst entscheiden darf, bleibt abzuwarten, ob der bestehende § 32 BDSG, der bislang den Umgang mit Beschäftigtendaten regelt, auch weiterhin gelten wird.

Künftig wird der Großteil der Datenverarbeitungen wohl auf Grundlage der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt. Interessenabwägungen sind stets subjektiv und lassen – je nach Position – die unterschiedlichsten Interpretationen zu. Unternehmen haben damit künftig mehr Argumentationsspielraum, müssen aber auch die daraus resultierende Rechtsunsicherheit in Kauf nehmen. In den Erwägungsgründen 47 ff. werden einzelne Beispiele genannt, in denen ein überwiegendes Interesse der verantwortlichen Stelle vorliegen soll, wie z.B. bei der Verhinderung von Betrug im erforderlichen Maße oder bei der Direktwerbung. Im letzteren Fall besteht – zur Wahrung der Rechte der Betroffenen – das Recht zum Widerspruch und die Pflicht zur Belehrung. Es ist davon auszugehen, dass neben den Datenschutzaufsichtsbehörden letztlich der EuGH als das für die Beurteilung der DSGVO zuständige Gericht die Auslegung von Art. 6 Abs. 1 lit. f DSGVO konkretisieren wird bzw. muss.

Besonders kritische Datenverarbeitungen, wie das Profiling, die massenhafte Verarbeitung sensitiver Daten oder die massenhafte Überwachung des öffentlichen Raums durch Videosysteme, unterliegen zudem einer Folgenabschätzung. Nach Art. 35 DSGVO ist diese vom Unternehmen durchzuführen, wenn Datenverarbeitungen ein erhöhtes Risiko für die Betroffenen nach sich ziehen. Zudem muss in bestimmten Fällen eine Konsultation der Aufsichtsbehörde erfolgen, Art. 36 DSGVO. Welche Verarbeitungen letztlich umfasst sein sollen, soll durch die Datenschutzaufsichtsbehörden konkretisiert werden.

b) Die Einwilligung als Rechtsgrundlage

Erwartungsgemäß ist auch die Einwilligung weiterhin als Grundlage für den Umgang mit Daten anerkannt. Die Voraussetzungen ergeben sich aus Art. 7 DSGVO. Im Einzelnen:

- **Form:** Es ist künftig keine spezielle Form der Einwilligung mehr vorgeschrieben, d.h. mündliche, elektronische und schriftliche Einwilligungen sind zulässig. Die Einwilligung muss in verständlicher und leicht zugänglicher Form zur Verfügung gestellt werden, Erwägungsgrund 42 DSGVO. Damit sind mündliche Einwilligungen eher kritisch.

- **Opt-In:** Das Opt-In, d.h. der Klick mit der Maus auf ein Kästchen, reicht künftig aus, um eine Einwilligung zu erteilen. Der Opt-Out ist hingegen grundsätzlich nicht mehr zulässig, so dass voreingestellte Klicks oder reine Widerspruchslösungen nicht mehr zulässig sind (siehe Erwägungsgrund 32 DSGVO). Da künftig bei Direktwerbung ein „berechtigtes“ Interesse von Unternehmen vorliegen soll und hier der Opt-Out in Form des Widerspruchsrechts noch möglich ist, ergeben sich gleichwohl Erleichterungen für Unternehmen.

- **Freiwilligkeit:** Kopplungen sind nicht zulässig, d.h. die Erfüllung eines Vertrages darf nicht von der Einwilligung abhängig gemacht werden, wenn diese nicht für die Erfüllung des Vertrages erforderlich ist. Der Praxis z.B. die Nutzung eines Webservices von der Einwilligung in die Nutzung von Daten in werbliche Zwecke abhängig zu machen, wird damit eine Absage erteilt. Die Einwilligung ist zudem bei einem eindeutigen Ungleichgewicht zwischen Betroffenem und Datenverarbeiter unzulässig. Damit sind sowohl Einwilligungen im Beschäftigungsverhältnis als auch Einwilligungen im Massenverkehr zwischen Verbrauchern und Unternehmen weiterhin risikobehaftet. Im letzteren Fall ist nie ganz auszuschließen, dass ein solches Ungleichgewicht insbesondere bei Marktführern anzunehmen ist.

- **Inhalt:** Die Einwilligung ist klar und leicht verständlich zu formulieren, es sind u.a. die verantwortliche Stelle, die Zwecke und Informationen über das Widerrufsrecht anzugeben. Für verschiedene Datenverarbeitungen sind verschiedene Einwilligungen einzuholen, damit der Betroffene sich frei entscheiden kann, in was er konkret einwilligt bzw. für welchen Zweck er die Einwilligung nicht erteilen möchte. Dies wird in der Praxis nicht leicht umsetzbar sein, da ggf. eine Vielzahl von Einwilligungen einzuholen ist. Ob die Voraussetzungen, deren Einhaltung die Rechtsprechung hinsichtlich der Konkretisierung des Inhalts der Einwilligung zurzeit in Deutschland einfordert, auf dem jetzigen Niveau bleiben oder ob aufgrund abweichender europäischer Praxis eine Absenkung dieser Standards erfolgen wird, bleibt abzuwarten.

- **Nachweis:** Unternehmen müssen nachweisen, dass die Einwilligung erteilt wurde. Wie der Nachweis geführt werden soll, ist nicht definiert. Eine umfassende Dokumentation ist allerdings empfehlenswert, da letztlich die Unternehmen für einen aufgrund einer fehlenden Einwilligung unzulässigen Umgang mit Daten haften.

c) Exkurs: Zulässigkeit von Big-Data-Anwendungen?

Entgegen den Erwartungen vieler Unternehmen gilt auch künftig das Prinzip der Zweckbindung, Art. 5 Abs. 1 lit. b, 6 Abs. 4 DSGVO. Hat ein Unternehmen Daten für Zwecke der Vertragserfüllung erhoben, darf es diese Daten nicht für Marketingzwecke nutzen oder für beliebige Zwecke, die es nicht bereits bei der Erhebung der Daten bereits festgelegt und transparent mitgeteilt hat. Eine Zweckänderung ist nur dann zulässig, wenn der neue Zweck mit dem alten Zweck vereinbar ist. Dies ist anhand verschiedener Kriterien zu bestimmen. Dabei sind insbesondere die folgenden Kriterien zu berücksichtigen:

- die Verbindung zwischen den Zwecken,

- der Gesamtkontext, in dem die Daten erhoben wurden,

- die Art der Daten,

- die möglichen Konsequenzen für die Betroffenen,

- die umgesetzten angemessenen technisch-organisatorischen Maßnahmen.

Im Ergebnis werden damit z.B. Big-Data-Anwendungen, in denen Daten zweckfrei in möglichst großen Mengen zusammengetragen und im Anschluss z.B. zur Gewinnung neuer Erkenntnisse ausgewertet werden, auch künftig kritisch zu wer-

ten sein. Da die o.g. Kriterien jedoch durchaus offene Interpretationen erlauben, wird hier abzuwarten sein, wie die Praxis den Zweckbindungsgrundsatz umsetzt.

Hieraus ergibt sich folgender Handlungsbedarf für die Unternehmen:

- Überprüfung der Rechtsgrundlagen bestehender Datenverarbeitungen im Unternehmen; ggf. Durchführung der Folgenabschätzung;
- Überprüfung des Umgangs mit pseudonymisierten Daten;
- Überprüfung und Anpassung von Vertragsvorlagen und Einwilligungserklärungen;
- Überprüfung der Dokumentation von Einwilligungserklärungen;
- Überprüfung und Anpassung bestehender Betriebsvereinbarungen unter Berücksichtigung der DSGVO.

2. Datenverarbeitung durch Dienstleister – Weiterhin zulässig?

a) Auftragsdatenverarbeitung

Eine weisungsgebundene Datenverarbeitung durch externe Dienstleister im Wege der Auftragsdatenverarbeitung (nun „Auftragsverarbeitung“) ist gem. Art. 28 DSGVO weiterhin zulässig. Die dem Auftragnehmer („Auftragsverarbeiter“) vertraglich aufzuerlegenden Pflichten gehen allerdings deutlich weiter als bisher: Neben der Durchführung von Maßnahmen zur Datensicherheit (insbesondere Verschlüsselung) muss der Auftragsverarbeiter nun sämtliche Mitarbeiter zur Verschwiegenheit verpflichten. Ihn treffen zudem umfangreichere Dokumentations- und Meldepflichten als bisher. Außerdem muss der Auftragsverarbeiter bei der Erfüllung von Betroffenenrechten mitwirken und gegebenenfalls mit der Aufsichtsbehörde kooperieren. Der bisher oft problematische Einsatz von Subunternehmern durch den Auftragsverarbeiter wird dahingehend geregelt, dass gem. Art. 28 Abs. 2 DSGVO die Einschaltung von Subunternehmern zukünftig nur noch mit vorheriger Einwilligung des Auftraggebers möglich ist.

Flankiert werden diese Maßnahmen durch eine Haftung des Auftragnehmers hinsichtlich seiner vorgenannten Pflichten. Verstößt er gegen Weisungen des Auftraggebers, ist er uneingeschränkt verantwortlich.

b) Cloud Services

Besondere Relevanz haben die neuen Änderungen für Cloud-Dienste, die im Regelfall als Auftragsdatenverarbeitung ausgestaltet sind: Der gesteigerte Pflichtenkreis des Cloud-Anbieters und die erforderliche Zusammenarbeit mit dem Cloud-Nutzer erfordern ggf. Anpassungen bestehender Verträge. Insbesondere zur Einschaltung von Subunternehmern fanden sich in der Praxis bisher oftmals weniger restriktive Regelungen.

c) Joint Controllers

Anders als bisher kann es nun dazu kommen, dass mehrere Beteiligte gleichrangig für die Verarbeitung personenbezogener Daten verantwortlich sind (sog. „Joint Controllers“), wenn sie die Zwecke und Mittel der Verarbeitung gemeinsam festlegen, Art. 26 Abs. 1 DSGVO. In diesem Szenario müssen vertragliche Regelungen dazu getroffen werden, wer welche datenschutzrechtlichen Verpflichtungen erfüllt; insbesondere im Hinblick auf die Betroffenenrechte. Das wesentliche der Vereinbarung muss den Betroffenen zudem gem. Art. 26 Abs. 3 DSGVO zur Verfügung gestellt werden, wobei noch unklar ist, wie weit diese Verpflichtung inhaltlich im Detail reicht.

Hieraus ergibt sich folgender Handlungsbedarf für die Unternehmen:

- Prüfung und ggf. Nachverhandlung bestehender ADV-Verträge;
- Sorgfältige Auswahl und Kontrolle des Auftragsverarbeiters anhand neuer Maßstäbe;
- Vorgänge identifizieren, bei denen eine gemeinsame Verarbeitung vorliegen könnte und ggf. entsprechende Vereinbarungen treffen.

3. Unsichere Drittstaaten, das Ende von Safe Habor und das neue EU-US Privacy Shield – Was nun bei internationalen Datentransfers?

Neue Regelungen ergeben sich im Bereich des internationalen Datentransfers, d.h. der Übermittlung von personenbezogenen Daten aus der EU in außereuropäische Drittstaaten.

Für US-Datentransfers hat der Europäische Gerichtshof (EuGH) bereits im Oktober 2015 die Entscheidung 2000/520/EG der Kommission zur Angemessenheit des Datenschutzniveaus bei sog. Safe Harbor zertifizierten US-Unternehmen für ungültig erklärt. Personenbezogene Daten dürfen auf dieser Grundlage nicht mehr in die USA übermittelt werden.

Das Nachfolgeabkommen, das ebenfalls auf einer Selbstregistrierung der Unternehmen basierende sog. EU-US Privacy Shield, befindet sich derzeit in der Abstimmung zwischen Kommission, Art. 29 Arbeitsgruppe und den Mitgliedsstaaten und kann vor Zustimmung des Parlaments zu dem entsprechenden Vorschlag der Kommission und Verabschiedung durch den Rat, die frühestens für Juni diesen Jahres erwartet wird, keine Rechtsgrundlage für US-Datenübermittlungen darstellen.

Fehlt ein Angemessenheitsbeschluss der Kommission und sind die einschlägigen Ausnahmetatbestände, wie z.B. Einwilligung des Betroffenen oder Übermittlung zur Erfüllung eines Vertrags, nicht einschlägig, bedarf es – wie bislang auch – geeigneter Garantien zur Legitimierung des Transfers. Zu dem Instrumentarium geeigneter Garantien, die keine Genehmigung der Aufsichtsbehörde im Einzelfall erfordern, zählen neben Binding Corporate Rules von der Kommission in einem Prüfverfahren genehmigte „Standarddatenschutzklauseln". Bis auf weiteres dürften die von der Kommission verabschiedeten Standardvertragsklauseln für Übermittlungen an Auftragsverarbeiter (Beschluss 2010/87/EU) und für Übermittlungen an verantwortliche Stellen (Entscheidung 2001/497/EG und Entscheidung 2004/915/EG betreffend die Einführung alternativer Standardvertragsklauseln) Standarddatenschutzklauseln in diesem Sinne darstellen.

Neu eingeführt wurde die Möglichkeit, von einer Aufsichtsbehörde erlassene Standarddatenschutzklauseln von der Kommission für die allgemeine Verwendung genehmigen zu lassen. Als geeignete Garantien anerkannt werden bei entsprechender Genehmigung zudem auch branchenbezogene Verhaltensregeln und sog. Zertifizierungsmechanismen. Alternativ kann sich ein Unternehmen – wie bisher auch – im Einzelfall die mit einem Datenimporteur im Drittland vereinbarten Vertragsklauseln als geeignete Garantien durch die zuständige Aufsichtsbehörde genehmigen lassen. Auch der Auftragsverarbeiter (und nicht nur der für die Verarbeitung Verantwortliche, wie es in der Vergangenheit erforderlich war) kann geeignete Garantien vereinbaren, was die Praxis der Einbindung von Unterauftragnehmern durch EWR-Auftragsverarbeiter erheblich vereinfachen sollte. Die Akzeptanz von Binding Corporate Rules soll durch die Konkretisierung der inhaltlichen Vorgaben insbesondere in Bezug auf Durchsetzbarkeit, Haftung und Verbindlichkeit gegenüber den teilnehmenden Unternehmen und die Vereinfachung des Genehmigungsverfahrens gestärkt werden.

Hieraus ergibt sich folgender Handlungsbedarf für die Unternehmen:

- Überprüfung der Leistungsbeziehungen zu Mitarbeitern, Kunden und Dienstleistern hinsichtlich relevanter Datenübermittlungen in Drittländer und Prüfung der Einhaltung der Voraussetzungen;

- Prüfung, ob die Erweiterung und die Flexibilisierung der geeigneten Garantien zur Legitimation von internationalen Transfers neue Gestaltungsspielräume eröffnen.

4. Aufsicht und Durchsetzung der DSGVO

Durch die DSGVO ändern sich behördliche Zuständigkeiten und mögliche Sanktionen im Falle von Datenschutzverstößen.

a) One-Stop-Shop

Bei grenzüberschreitenden Datenverarbeitungen sind bislang mitunter mehrere Datenschutzbehörden gleichberechtigt nebeneinander zuständig. Dies soll sich zukünftig ändern: Die Funktion einer „federführenden Aufsichtsbehörde" übernimmt die Aufsichtsbehörde, die in dem Gebiet zuständig ist, in dem das betreffende Unternehmen seine Hauptniederlassung oder einzige Niederlassung innerhalb der EU hat (Art. 56 DSGVO). Aufsichtsbehörden aus anderen Mitgliedsstaaten können „betroffene Aufsichtsbehörden" sein, die von der federführenden Aufsichtsbehörde im Rahmen eines Verfahrens zu involvieren sind. Am Ende soll jedoch eine einheitliche Entscheidung stehen, an die alle Aufsichtsbehörden gebunden sind (Art. 60 ff. DSGVO).

Darüber hinaus gibt es zukünftig das sogenannte „Kohärenzverfahren" (Art. 63 ff. DSGVO). Im Rahmen des Kohärenzverfahrens wird ein sog. „Europäischer Datenschutzausschuss" verbindliche Stellungnahmen abgeben, die innerhalb der EU von den Aufsichtsbehörden zu beachten sind. Der Europäische Datenschutzausschuss löst die Arbeit der bisherigen Artikel-29-Arbeitsgruppe ab, deren Stellungnahmen nicht verbindlich sind. Der Europäische Datenschutzausschuss wird unter anderem aus Vertretern der nationalen Aufsichtsbehörden sämtlicher Mitgliedsstaaten der EU bestehen.

b) Schärfere Sanktionen und Verbandsklagerecht

Geldbußen sollen „wirksam, verhältnismäßig und abschreckend" sein. Dies wird durch einen im Vergleich zur jetzigen Rechtslage maßgeblich erhöhten Bußgeldrahmen sichergestellt. Künftig können Bußgelder bis zu EUR 20 Millionen bzw.

bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens verhängt werden.

Darüber hinaus kommen zivilrechtliche (z.B. Schadensersatz) und strafrechtliche Konsequenzen in Betracht. Insbesondere sieht die DSGVO ein Verbandsklagerecht vor. Rechte der Betroffenen können somit künftig z.B. durch Verbraucherschutzverbände geltend gemacht werden, Art. 80 DSGVO. Über das gerade in Deutschland in Kraft getretene Unterlassungsklagegesetz hinaus können diese nach der DSGVO z.B. auch Löschungs- oder Schadenersatzansprüche der Betroffenen einklagen.

5. Datenschutzorganisation im Unternehmen – Neue Herausforderungen?

Die DSGVO dient zum einen der Verringerung bürokratischer Hürden. Zum anderen soll die Datenschutzorganisation in Unternehmen für Außenstehende sowie Aufsichtsbehörden transparenter werden. Dies führt insbesondere zu folgenden Änderungen:

a) Betrieblicher Datenschutzbeauftragter

Nach Art. 37 Abs. 1 DSGVO muss bei Unternehmen in der Privatwirtschaft zukünftig ein betrieblicher Datenschutzbeauftragter jedenfalls dann bestellt werden, wenn

- die Kerntätigkeit als verantwortlichen Stelle oder des Auftragsverarbeiters eine umfangreiche, regelmäßige und systematische Beobachtung der Betroffenen erforderlich machen, oder
- wenn die Kerntätigkeit der verantwortlichen Stelle die Verarbeitung sensibler Daten umfasst.

Es ist bereits jetzt absehbar, dass der deutsche Gesetzgeber von der Befugnis in Art. 37 Abs. 4 DSGVO Gebrauch machen und weitere Fälle vorschreiben wird, in denen zwingend ein Datenschutzbeauftragter zu benennen ist, sodass die bislang geltenden Regelungen weiterhin gelten.

Nach der DSGVO ist es zukünftig auch möglich, einen gemeinsamen Datenschutzbeauftragten für eine Unternehmensgruppe bzw.einen Konzern zu ernennen, sofern dieser leicht erreichbar für die einzelnen Unternehmen bzw. Niederlassungen ist (Art. 37 Abs. 2 DSGVO). Der Konzerndatenschutzbeauftragte, der bislang nicht im deutschen Recht verankert war, bekommt damit eine eigenständige Funktion.

b) Neue Dokumentations- und Meldepflichten

Nach der bislang geltenden EU-Datenschutz-Richtlinie ist es grundsätzlich erforderlich, neue Datenverarbeitungsverfahren an die zuständigen Aufsichtsbehörden zu melden. In Deutschland ist diese Meldung entbehrlich, sofern ein betrieblicher Datenschutzbeauftragter bestellt ist. Die DSGVO verzichtet auf starre Meldepflichten, erhöht allerdings im Gegenzug die Dokumentations- und Meldepflichten, die – je nach Risiko eines bestimmten Datenverarbeitungsprozesses – umzusetzen sind (sog. „Risikoansatz“). Deutsche Unternehmen müssen sich insofern erheblich umstellen. Dazu gehören unter anderem:

- Erstellung von Verzeichnissen von Verarbeitungstätigkeiten (Artikel 30 DSGVO), die im Wesentlichen den bereits jetzt verpflichtend vorgesehenen Verfahrensverzeichnissen entsprechen. Diese Verpflichtung trifft alle Unternehmen, es sei denn sie beschäftigen weniger als 250 Mitarbeiter und betreiben keine kritischen Datenverarbeitungen. Die Regelung gilt künftig auch für Auftragsverarbeiter.
- Durchführung von Datenschutzfolgeabschätzungen, teilweise unter Einbindung der Aufsichtsbehörden (Art. 35 DSGVO), wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge hat.
- Meldungen von Datenschutzverletzungen an die Aufsichtsbehörde (Art. 33 DSGVO); es sei denn, dass die Datenschutzverletzung voraussichtlich kein Risiko für die persönlichen Rechte und Freiheiten der Betroffenen bedeutet.
- Benachrichtigung der von einer Datenschutzverletzung betroffenen Personen (Art. 34 DSGVO), wenn wahrscheinlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen besteht.

Dabei wurden die Meldepflichten bei Datenschutzverletzungen erheblich verschärft: Die Meldung über eine Datenschutzpanne muss gegenüber der zuständigen Aufsichtsbehörde grundsätzlich innerhalb von 72 Stunden nach Kenntniserlangung erfolgen. Auch die Meldung an die Betroffenen unterliegt Fristen. Im Gegensatz zum heutigen § 42a BDSG sehen Art. 33, 34 DSGVO bereits eine Meldepflicht bei der „Verletzung des Schutzes personenbezogener Daten“ vor. Umfasst ist künftig nach Art. 4 Nr. 12 DSGVO z.B. bereits die unbeabsichtigte Offenlegung von Daten gegenüber unbefugten Dritten.

c) Datensicherheit

Nach der DSGVO haben sowohl die verantwortliche Stelle als auch der Auftragsverarbeiter die technischen und organisatorischen Maßnahmen zu schaffen, die in Anbetracht des konkreten Risikos ein angemessenes Schutzniveau gewährleisten. Dabei werden Maßnahmen verlangt, die in wesentlichen Teilen bereits nach § 9 BDSG vorausgesetzt werden. Hierzu gehören:

- Pseudonymisierung und Verschlüsslung personenbezogener Daten;
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, mit denen personenbezogene Daten verarbeitet werden;
- Möglichkeit der raschen Wiederherstellung verlorener Daten nach einem technischen Zwischenfall;
- Etablierung von Verfahren zum regelmäßigen Monitoring der Wirksamkeit eingerichteter technischer und organisatorischer Maßnahmen.

Die DSGVO verlangt nicht, dass sämtliche Maßnahmen in jedem Fall bestmöglich umgesetzt werden. Die zu treffenden Maßnahmen sind vielmehr danach auszurichten, welche Risiken jeweils in Bezug auf die konkret betroffenen personenbezogenen Daten drohen können. Auch hier gilt also der sogenannte „Risikoansatz“. Die DSGVO verlangt eine regelmäßige Kontrolle und einen Nachweis der Umsetzung der Maßnahmen. Hier werden sich viele Unternehmen umstellen müssen.

Zudem gelten nach der DSGVO höhere Anforderungen für Unternehmen im Hinblick auf Entwicklung und Installation von IT-Systemen. So ist bereits bei der Entwicklung von Software darauf zu achten ist, dass die Grundsätze der Datensparsamkeit bestmöglich zur Geltung kommen („privacy by design“). Darüber hinaus sollte jegliche Software (also auch eingekaufte Standardsoftware) so customized bzw. bei Installation so eingestellt werden, dass deren Benutzer keine unnötigen personenbezogenen Daten erheben oder verarbeiten („privacy by default“).

Hieraus ergibt sich folgender Handlungsbedarf für Unternehmen:

- Prüfung, ob ein Datenschutzbeauftragter bestellt werden muss und ggf. Bestellung, sofern noch nicht erfolgt;
- Prüfung und Implementierung von Prozessen, die die erweiterten Dokumentations- und Meldepflichten sicherstellen;
- Prüfung, ob Folgenabschätzungen durchzuführen sind;
- Prüfung, ob die Systeme die Anforderungen von privacy by design und default umsetzen;
- Einführung von Prozessen zur Implementierung und regelmäßigen Kontrolle der erforderlichen technisch-organisatorischen Maßnahmen.

6. Von der Mutter zur Tochter zur Schwester – Wie geht Datenschutz im Konzern?

Die vielfach gewünschte Privilegierung von konzern- oder gruppeninternen Datenübermittlungen wurde nicht umgesetzt. Erleichterungen für Konzerngestaltungen ergeben sich aber aus der ausdrücklichen Anerkennung der Position eines gemeinsamen Datenschutzbeauftragten für eine Unternehmensgruppe sowie der Vereinfachung der Zuständigkeiten für die Überwachung der Datenschutz-Compliance („One-Stop-Shop“).

Hieraus ergibt sich folgender Handlungsbedarf für die Unternehmen:

- Identifizierung der Datenübermittlungen in Drittländer auch bei konzerninternen Leistungsbeziehungen und Verifizierung der rechtlichen Grundlage;
- Prüfung, ob die Einführung von Binding Corporate Rules eine Alternative zur Legitimierung der Datenübermittlungen und zur Vereinfachung der Abläufe und der vertraglichen Dokumentation darstellt; dies empfiehlt sich insbesondere bei konzerninternen Service-Strukturen;
- Anpassung der Datenschutz-Compliance Organisation;
- Zuweisung der Zuständigkeiten und Verantwortlichkeiten entsprechend den Vorgaben der DSGVO.

7. Einführung neuer Betroffenenrechte

Die Rechte der Betroffenen werden erweitert. Einige neue Rechte kommen hinzu, die seitens der Unternehmen umzusetzen sind:

a) Neu: Recht auf Datenportabilität

Zukünftig kann ein Betroffener von einer verantwortlichen Stelle verlangen, dass die personenbezogenen Daten, die der Betroffene dem Unternehmen zur Verfügung gestellt hat, dem Betroffenen in einem gängigen elektronischen Format zur Verfügung gestellt werden (Art. 20 DSGVO). Soweit technisch möglich, ist das Unternehmen darüber hinaus verpflichtet, diese Daten an einen neuen Anbieter zu übermitteln, damit dieser die Daten gleich bei sich im System einpflegen kann. Hier sind technische Hindernisse zu erwarten: Unternehmen arbeiten üblicherweise mit verschiedenen IT-Systemen, aus denen sich nicht ohne weiteres sämtliche bereitgestellten Daten „auf Knopfdruck" extrahieren und in einem gängigen Datenformat zusammenfassen lassen. Die Umsetzung dieser Anforderung erfordert daher die Umsetzung von entsprechenden technischen Vorkehrungen.

b) Pflicht zur transparenten Information

Die bereits jetzt bestehenden Informationspflichten werden erweitert (Art. 12 bis 14 DSGVO). Neben den bereits heute gegenüber den Betroffenen zu erteilenden Informationen, wie Angaben zur verantwortlichen Stelle, Umgang mit den Daten oder Widerspruchsrechte, ist zukünftig u.a. auf Folgendes hinzuweisen:

- Sofern die Rechtsgrundlage auf einer Interessenabwägung beruht, Informationen über die berechtigten Interessen der verantwortlichen Stelle;
- Die Speicherdauer der personenbezogenen Daten (soweit möglich);
- Das Bestehen eines Beschwerderechts des Betroffenen gegenüber einer Aufsichtsbehörde;
- Die Übermittlung von Daten an einen Empfänger mit Sitz in einem Drittland und ob im Hinblick auf dieses Drittland ein sogenannter „Angemessenheitsbeschluss" der Kommission vorliegt oder ob auf andere Weise ein angemessener Datenschutzstandard gewährleistet wird.

Diese Informationen sind grundsätzlich bei der Erhebung bzw. bei einer Änderung der Zwecke im Umgang mit den Daten gegenüber dem Betroffenen zu erteilen. Werden Daten nicht direkt bei dem Betroffenen erhoben (z.B. im Rahmen der bislang nicht erlaubten Freundschaftswerbung), ist auch dieser zu informieren. Die Information muss zudem leicht verständlich sein; es bleibt abzuwarten, ob die EU-Kommission von ihrer Befugnis Gebrauch macht, Bildsymbole vorzugeben, die die Information erleichtern sollen.

c) Weitergehendes Widerspruchsrecht der Betroffenen

Die bislang bestehenden Widerspruchsrechte im Umgang mit Daten werden ausgeweitet (Art. 21 DSGVO) Zukünftig können Betroffene z.B. Widerspruch gegen eine auf einer Interessenabwägung beruhenden Verarbeitung ihrer Daten nach Art. 6 Abs. 1 lit. f DSGVO einlegen, sofern Gründe vorliegen, die sich aus ihrer besonderen persönlichen Situation ergeben. Sofern die verantwortliche Stelle „zwingende schutzwürdige" Gründe für die Verarbeitung „nachweisen" kann, darf sie die Daten weiterhin verarbeiten. Hier bleibt abzuwarten, wie sich dieses Recht in der Praxis auswirkt und welche Begründungen bzw. Nachweise hier letztlich seitens der Behörden anerkannt werden. Zudem bestehen Widerspruchsrechte gegen Direktmarketingmaßnahmen bzw. Profiling, die keiner weiteren Bedingung unterliegen.

d) Recht auf Vergessenwerden

Die DSGVO sieht nun explizit ein „Recht auf Vergessenwerden" vor. Diejenigen, die mit dem deutschen Datenschutzrecht vertraut sind, wird ein solches Recht nicht überraschen. Es ist weitgehend deckungsgleich mit den bereits nach dem BDSG etablierten Löschungsansprüchen. Es gibt jedoch auch einige Erweiterungen: Hat die verantwortliche Stelle die personenbezogenen Daten öffentlich gemacht (z.B. auf einer Website), so ist die verantwortliche Stelle zukünftig auch verpflichtet, Dritte darüber zu informieren, dass ein Betroffener die Löschung sämtlicher Links zu diesen personenbezogenen Daten und deren Kopien und Replikationen verlangt hat. Wie diese Informationen erfolgen sollen, ist derzeit noch unklar.

Hieraus ergibt sich folgender Handlungsbedarf für die Unternehmen:

- Prüfung, in welchen Fällen unternehmensintern das Recht auf Datenportabilität greift, d.h. welche Systeme und welche personenbezogenen Daten der Betroffenen sind erfasst;
- Prüfung, welches Datenformat für die Bereitstellung dieser Daten geeignet ist;
- Prüfung, ob dieses Datenformat „gängig" im Sinne der DSGVO ist;
- Überprüfung und Vervollständigung der bereits bestehenden Datenschutzpolicies, Einwilligungserklärungen etc.;
- Prüfung und Implementierung von Prozessen zur Mitteilung der Informationen (insbesondere bei Zweckänderungen und Erhebungen über Dritte);

- Dokumentation der berechtigten Interessen und Implementierung von Prozessen im Umgang mit Widersprüchen;
- Einführung von Prozessen im Umgang mit dem Recht auf Vergessenwerden.

Veranstaltungshinweise

Wir laden Sie herzlich zu den Veranstaltungen der Luther Vortragsreihe zu den Auswirkungen der neuen EU-Datenschutzgrundverordnung auf die Datenverarbeitung in Unternehmen ein. Dort stellen wir Ihnen die Regelungen detailliert vor. Unsere Veranstaltungen finden in unseren jeweiligen Büros zu folgenden Terminen statt:

- Essen: 28. April 2016, 9:30-12:00 Uhr;
- Köln: 2. Juni 2016, 14:00-18:00 Uhr;
- Hamburg: 8. Juni 2016, 9:00-12:00 Uhr;
- Hannover: 15. Juni 2016, 9:00-12:00 Uhr;
- Frankfurt: 5. Juli 2016, 9:00-12:00 Uhr.

Weitere Veranstaltungen dieser Reihe in Stuttgart (19. Juli 2016) und Berlin (29. September 2016) sind in Planung; eine Anmeldung dazu ist in Kürze möglich.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Silvia C. Bauer, Partnerin
Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22
50678 Köln, Telefon +49 221 9937 25789
silvia.c.bauer@luther-lawfirm.com

Checkliste für Unternehmen

Prüfen Sie anhand der nachfolgenden Checkliste, ob Sie bereits die Vorgaben der neuen EU-DSGVO umsetzen oder ob noch Handlungsbedarf besteht:

1. Rechtsgrundlagen der Datenverarbeitung

- ❑ Besteht für jede Datenverarbeitung eine Erlaubnisgrundlage und ist diese hinreichend dokumentiert, insbesondere:
  - ❑ Sind Einwilligungserklärungen klar und leicht verständlich formuliert und nachweisbar?
  - ❑ Ist im Falle von Datenverarbeitungen, die aufgrund einer Interessenabwägung stattfinden, nachvollziehbar dokumentiert, dass eine Interessenabwägung durchgeführt wurde und welche Interessen in die Abwägung eingestellt wurden?
  - ❑ Werden die Sondervorschriften für die Verarbeitung von besonderen personenbezogenen Daten, wie z.B. Gesundheit, Religion oder Rasse, beachtet?
  - ❑ Ist sichergestellt, dass im Falle besonders kritischer Datenverarbeitungen, wie dem Profiling, eine Folgenabschätzung durchgeführt wird?
  - ❑ Sofern Datenverarbeitungen gemeinsam mit anderen verantwortlichen Stellen vorgenommen werden („Joint Controllers“), ist die Verantwortlichkeit im Innenverhältnis vertraglich geregelt?

2. Datenverarbeitung durch Dienstleister

- ❑ Entsprechen die mit Auftragsverarbeitern abgeschlossenen Verträge den gesteigerten gesetzlichen Anforderungen?
- ❑ Ist sichergestellt, dass auch Auftragsverarbeiter zukünftig Verfahrensverzeichnisse gemäß der Anforderungen der DSGVO erstellen?
- ❑ Ist eine ausreichende Kontrolle der Dienstleister am modifizierten Maßstab gewährleistet?
- ❑ Erfüllen genutzte Cloud-Dienste die modifizierten Anforderungen, insbesondere im Hinblick auf den Einsatz von Subunternehmern?
- ❑ Ist sichergestellt, dass ein etwaiger Datentransfer in die USA nicht länger auf der Basis von Safe Harbor, sondern auf geeigneten alternativen Garantien, insbesondere den Standardvertragsklauseln, stattfindet?

3. Datenschutz im Unternehmen

- ❑ Werden die Anforderungen an die Dokumentation der Datenverarbeitungen bzw. der IT-Systeme bereits erfüllt?
- ❑ Ist ein Verfahren vorgesehen, mit dem sichergestellt wird, dass Datenschutzpannen in der Regel innerhalb der gesetzten Fristen der zuständigen Aufsichtsbehörde bzw. den Betroffenen gemeldet werden können?
- ❑ Sind Prozesse etabliert, die sicherstellen, dass bereits im Stadium der Entwicklung von IT-Systemen und Software der Grundsatz der Datensparsamkeit hinreichend berücksichtigt wird, um sicherzustellen, dass beim späteren Einsatz der Systeme nur die notwendigen personenbezogenen Daten verarbeitet werden („privacy by design“)?
- ❑ Sind Prozesse vorgesehen, die sicherstellen, dass IT-Systeme und Software so (vor-)konfiguriert sind, dass personenbezogene Daten nur in dem tatsächlich erforderlichen Umfang verarbeitet werden („privacy by default“)?
- ❑ Sind die konzerninternen Datenaustauschprozesse dokumentiert und bestehen entsprechende Rechtsgrundlagen insbesondere in Form von Auftragsverarbeiterverträgen oder Standardvertragsklauseln?

4. Betroffenenrechte

- ❑ Können die personenbezogenen Daten, die von dem neuen „Recht auf Datenportabilität“ erfasst sind, dem jeweiligen Betroffenen tatsächlich in einem „gängigen“ Dateiformat in elektronischer Form zur Verfügung gestellt werden?
- ❑ Werden die Betroffenen ausreichend und transparent informiert, insbesondere auch über die Speicherdauer der personenbezogenen Daten, das Beschwerderecht gegenüber einer Aufsichtsbehörde und über einen möglichen Drittlandsbezug?
- ❑ Sind Prozesse umgesetzt, die die Umsetzung des Rechts auf Vergessenwerden sicherstellen?

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapur, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com.

Auf den Punkt. Luther.