SKW
Schwarz
Rechtsanwälte

Practice Group IT & Digital Business
IT-Ticker – Sonderausgabe

EU-Datenschutz-Grundverordnung

Eine erste Einführung in die wesentlichen Neuerungen gegenüber dem geltenden deutschen Recht

Inhalt

Stand der Bearbeitung: 14. März 2016 © SKW Schwarz 2016

Autoren: Nikolaus Bertermann, Florian Hensel, Dr. Oliver Hornung, Franziska Ladiges, Daniel Meßmer, Dr. Matthias Nordmann M.A., Dr. Andreas Peschel-Mehner, Daniel Pfeifer, Sven Preiss LL.M., Stefan Schicker, Martin Schweinoch
Redaktionell Verantwortlicher: Nikolaus Bertermann. Leiter der Practice Group IT & Digital Business: Martin Schweinoch
E-Mail: IT-Ticker@skwschwarz.de

SKW Schwarz Rechtsanwälte Steuerberater Wirtschaftsprüfer Partnerschaft mbB
Eingetragen beim Amtsgericht München PR 884, Sitz der Partnerschaft ist München.
Vertretungsberechtigte: Markus von Fuchs LL.M., Andreas Seidel.

10719 **Berlin**
Kurfürstendamm 21
T 030 / 889 26 50-0
F 030 / 889 26 50-10

40212 **Düsseldorf**
Steinstraße 1/Kö
T 0221 / 82 89 59-0
F 0221 / 82 89 59-60

60598 **Frankfurt/Main**
Mörfelder Landstr. 117
T 069 / 63 00 01-0
F 069 / 63 55 22

20095 **Hamburg**
Ferdinandstraße 3
T 040 / 33 40 1-0
F 040 / 33 40 15 30

80333 **München**
Wittelsbacherplatz 1
T 089 / 286 40-0
F 089 / 280 94 32

Zusammenfassung

Die Datenschutz-Grundverordnung (DSGVO) wird voraussichtlich im Frühjahr 2018 in Kraft treten. Sie wird ohne nationale Umsetzungsakte unmittelbar geltendes Recht in allen Mitgliedsstaaten der EU. Zwar wird die DSGVO erheblich zur Harmonisierung des Datenschutzrechts in Europa beitragen, die ursprünglich geplante Vollharmonisierung ist aber durch zahlreiche Öffnungsklauseln nicht erreicht worden. Öffnungsklauseln gibt es beispielsweise im Beschäftigtendatenschutz und bei den Regelungen für den betrieblichen Datenschutzbeauftragten.

Der bereits aus der EU-Richtlinie von 1995 bekannte Grundsatz, dass jede Verarbeitung personenbezogener Daten grundsätzlich verboten ist, sofern sie nicht durch Gesetz, Rechtsverordnung oder die Einwilligung des Betroffenen erlaubt ist („Verbot mit Erlaubnisvorbehalt"), bleibt bestehen. Viele Pflichten in der DSGVO sind vergleichbar mit den aktuellen Regelungen im BDSG. Zahlreiche neue Begriffe und Regelungen werden voraussichtlich zunächst zu mehr Unsicherheit beim Umgang mit personenbezogenen Daten führen.

Ein Ziel der DSGVO ist die Stärkung der Betroffenenrechte. So sind die Dokumentationspflichten gestiegen und die Selbstbestimmungsrechte der Betroffenen gestärkt worden. Bei Verarbeitungen, die aufgrund einer positiven Interessenabwägung zugunsten des Unternehmens durchgeführt werden, besteht zukünftig ein ausdrückliches Widerspruchsrecht des Betroffenen. Unternehmen müssen vor der Verarbeitung personenbezogener Daten eine so genannte Datenschutzfolgeabschätzungen durchführen und unter Umständen die zuständige Aufsichtsbehörde konsultieren, die die Verarbeitung untersagen kann. Bei Datenschutzverletzungen bestehen umfassende Informations- und Dokumentationspflichten.

Der Bußgeldrahmen wurde deutlich erhöht und reicht jetzt bis zu 10 Mio€ oder 4% des weltweiten Jahresumsatzes der Unternehmensgruppe.

Die DSGVO gilt mit Inkrafttreten auch für Unternehmen, die zwar keine Niederlassung in der EU unterhalten, aber ihre Leistungen in der EU anbieten. Solche Unternehmen benötigen zukünftig einen benannten Vertreter innerhalb der EU.

Unternehmen müssen zukünftig Voreinstellungen und Produkte so gestalten, dass möglichst wenige personenbezogene Daten erhoben und verarbeitet werden („Privacy by Design").

Bei der Auftragsdatenverarbeitung bleiben die Regelungen im Kern gleich, die Verträge müssen aber an neue Begrifflichkeiten und Vorgaben angepasst werden. Die Auftragserteilung kann auch in elektronischer Form erfolgen. Prinzipiell wird eine Auftragsdatenverarbeitung auch in einem Drittstaat möglich sein.

Die Vorgaben für Datentransfers in Drittländer bleiben im Wesentlichen gleich, allerdings entfällt die im BDSG vorgesehene zweistufige Angemessenheitsprüfung.

Ein betrieblicher Datenschutzbeauftragter ist europaweit nur bei risikoträchtigen Verarbeitungen vorgeschrieben, strengere nationale Regelungen sind erlaubt.

Verbände können Regeln für branchenspezifische Datenverarbeitungen aufstellen und von den Aufsichtsbehörden freigeben lassen. Die DSGVO will die Zertifizierung von Verarbeitungen fördern und stellt klare Vorgaben dafür auf.

Die Datenschutzaufsicht bleibt national, bei Unternehmen mit mehreren Niederlassungen in der EU wird eine Aufsichtsbehörde federführend, aber nicht allein entscheidungsbefugt. Insgesamt sollen sich die Behörden bei vielen Entscheidungen und Regelungen intensiv miteinander abstimmen (Kohärenzpflicht).

1. Entwicklung und Inkrafttreten

Die EU-Kommission, der Rat und das Parlament der EU haben am 15.12.2015 eine politische Einigung über die lange geplante Datenschutz-Grundverordnung (DSGVO) erzielt. Parallel dazu wurde auch eine Einigung über eine Richtlinie für den Datenschutz bei der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erzielt. Die DSGVO und die parallele Richtlinie müssen noch durch die zuständigen Gremien auf EU-Ebene verabschiedet werden. Die Richtlinie ist dann – anders als die DSGVO – durch die Mitgliedsstaaten in nationales Recht umzusetzen.

Die DSGVO wird zwei Jahre und 20 Tage nach Verkündung in der gesamten EU unmittelbar geltendes Recht. Die DSGVO enthält ganz überwiegend unmittelbar anwendbare Regelungen. In einzelnen Themen wird entweder die EU-Kommission zum Erlass delegierter Rechtsakte ermächtigt oder die EU-Staaten können Regelungsspielräume nutzen. Der Datenschutz in der EU wird dadurch ganz wesentlich vereinheitlicht, aber nicht ganz vollständig.

Die DSGVO bringt auch eine ganze Reihe von sprachlichen Änderungen mit sich, wobei damit nicht immer auch eine Änderung der Bedeutung einhergeht. Beispielsweise wird aus der „verantwortlichen Stelle“ (BDSG) zukünftig „der für die Verarbeitung Verantwortliche“.

2. Allgemeine Bestimmungen und Grundsätze

Zwar werden viele in Deutschland bekannte Grundsätze beibehalten und weiterentwickelt. Die genaue Umsetzung unterscheidet sich allerdings oft von der aktuellen Situation. Die DSGVO enthält darüber hinaus wesentliche neue Elemente und Regelungsinhalte.

Die DSGVO gilt für alle für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter in der EU. Sie gilt aber auch für Leistungsangebote oder Verhaltensbeobachtungen in die EU durch Datenverarbeiter außerhalb der EU. Nicht von der DSGVO erfasst werden die Strafverfolgung und die EU selbst sowie rein persönliche oder familiäre Tätigkeiten.

Die immer noch umstrittene Frage, wann es sich genau um geschützte personenbezogene Daten handelt, beantwortet auch die DSGVO nicht präzise. Die bisherigen Unsicherheiten im Detail werden also nicht sicher ausgeräumt. Neu ist eine gemeinsame Verantwortung für personenbezogene Daten durch mehrere Stellen. Ebenfalls neu die der Begriff des Profiling um personenbezogene Aspekte zu analysieren oder vorherzusagen.

Ein für die Verarbeitung Verantwortlicher ist allgemein für die Einhaltung mehrerer Grundsätze für personenbezogene Daten rechenschaftspflichtig: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.

Für den Umgang mit personenbezogenen Daten bleibt es bei dem Verbotsprinzip: Der Umgang mit personenbezogenen Daten ist verboten, außer soweit er nach der DSGVO rechtmäßig ist. Wichtigste Rechtmäßigkeitsalternativen sind: eine Einwilligung des Betroffenen, die Vertragserfüllung oder vorvertragliche Maßnahmen, die Umsetzung rechtlicher Verpflichtungen, die Wahrnehmung berechtigter Interessen soweit nicht die Interessen des Betroffenen überwiegen.

Für eine Einwilligung ist eine informierte, freiwillige und unmissverständliche Willensbekundung des Betroffenen erforderlich. Eine bestimmte Form ist – anders als derzeit im BDSG – nicht vorgeschrieben. Die Einwilligung ist jederzeit frei widerruflich mit Wirkung für die Zukunft. Ein für die Verarbeitung Verantwortlicher muss das Vorliegen einer Einwilligung nachweisen können.

Die Verarbeitung besonderer Kategorien personenbezogener Daten (etwa über ethnische Herkunft, Religion, Gesundheit, biometrische Merkmale oder Sexualleben) ist nur unter besonderen Voraussetzungen zulässig. Besondere Einschränkungen gelten auch für Daten über strafrechtliche Verurteilungen oder Straftaten.

3. Rechte der betroffenen Personen

Aufgrund des bestehenden hohen Datenschutzniveaus in Deutschland fällt die Stärkung der Betroffenenrechte in Deutschland eher gering aus. Im Einzelnen:

a) Informationspflichten

Zukünftig sind Betroffene ausführlich schriftlich oder in elektronischer Form zu informieren, wenn personenbezogene Daten erhoben werden. In Bezug auf den Zeitpunkt und den Umfang der zu erteilenden Informationen wird zwischen der Erhebung bei dem Betroffenen und der Erhebung nicht bei dem Betroffenen unterschieden. Neben den allgemeinen Informationen, z.B. Informationen zu dem für die Verarbeitung Verantwortlichen oder Datenkategorien, sind Informationen zu erteilen, welche eine faire und transparente Verarbeitung gewährleisten sollen, z.B. Dauer der Datenspeicherung.

Zwar waren Unterrichtungspflichten auch bisher bekannt, Unternehmen sollten jedoch prüfen, ob ihre Datenschutzerklärungen und sonstigen Informationen, den neuen Informationspflichten gerecht werden und diese gegebenenfalls anpassen.

b) Auskunft, Berichtigung und Einschränkung der Verarbeitung

Neben den Informationspflichten über die Datenerhebung stehen Betroffenen wie bisher auch Auskunfts- und Berichtigungsrechte gegenüber dem für die Verarbeitung Verantwortlichen zu. Im Gegensatz zu den bestehenden Regelungen gibt es in Bezug auf den Umfang der Auskunft keine Differenzierung mehr nach Art des für die Verarbeitung Verantwortlichen. Jeden Verantwortlichen treffen somit die gleichen Auskunftspflichten. Für die Mehrzahl der Unternehmen bedeutet dies, dass die Auskünfte in Zukunft umfangreicher erfolgen müssen. Der Auskunftsprozess sollte entsprechend umgestellt werden.

Zudem kann der Betroffene in bestimmten Fällen eine Einschränkung der Verarbeitung seiner Daten verlangen. Dies ist mit der bisher bestehenden Möglichkeit der Sperrung von Daten zu vergleichen und somit keine wirkliche Neuerung im deutschen Recht.

Der für die Verarbeitung Verantwortliche hat Empfängern von Daten jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen.

c) Transparenz

Schon bisher wurde die Transparenz im Bereich des Datenschutzes groß geschrieben. Nunmehr ist dieser Grundsatz ausdrücklich in die DSGVO aufgenommen worden. Sämtliche Informationen und Auskünfte sind danach

schriftlich, leicht verständlich und in der Regel unentgeltlich zu erteilen. Die Auskunft sollte in der Regel spätestens einen Monat nach dem Antragseingang erfolgen.

d) Recht auf „Vergessenwerden“

In erster Linie betrifft das Recht auf „Vergessenwerden“ das schon bislang zumindest in Deutschland existierende Recht auf Datenlöschung, wenn die Speicherung der Daten nicht aus zwingenden rechtlichen oder vertraglichen Gründen erforderlich ist. Die Regelung enthält sowohl eine Aufzählung von Fällen, in denen die Löschung erfolgen muss als auch eine Aufzählung, in denen die Verarbeitung trotz Löschungsbegehren weiterhin zulässig ist.

Wirklich neu ist die Regelung, dass Anbieter, welche personenbezogene Daten öffentlich machen, nunmehr verpflichtet werden, Dritte, welche die Daten verarbeiten über das Löschungsbegehren zu informieren. Dies betrifft vor allem Social Media Anbieter wie Facebook, welche zukünftig Sorge tragen müssen, dass auch Verlinkungen durch Dritte auf gelöschte Inhalte entfernt werden.

e) Datenübertragbarkeit

Neu ist das Recht der Betroffenen, die Herausgabe ihrer zur Verfügung gestellten Daten in einem üblichen maschinenlesbaren Format zu verlangen. Dieses Recht können Betroffene immer dann geltend machen, wenn die Datenverarbeitung allein auf einer Einwilligung oder einem Vertrag beruht. Ziel ist es, den Betroffenen einen reibungslosen Umzug zu einem anderen Provider zu ermöglichen.

Deutlich wird, dass dieses Recht vor allem auf Social Media Anbieter, wie z.B. Facebook abzielt. Da eine Einschränkung des Rechts jedoch nicht vorgesehen ist, können auch kleinere Anbieter wie z.B. Anbieter von TV-Decodern, auf welchem Präferenzen des Nutzers gespeichert sind, von diesem Recht betroffen sein. Es bleibt abzuwarten, wie häufig und umfangreich Betroffene von diesem Recht Gebrauch machen werden und welchen Aufwand dies bei den Dienstleistern verursachen wird.

f) Widerspruchsrecht

Sofern die Datenerhebung und -verarbeitung aufgrund einer positiven Interessenabwägung für den für die Verarbeitung Verantwortlichen erfolgt, hat der Betroffene ein jederzeitiges Widerspruchsrecht. In Bezug auf Direktwerbung gibt es ein Widerspruchsrecht unabhängig von der Art der Datenerhebung. Für deutsche Verhältnisse neu an dieser Regelung ist allein die Formulierung in der Verordnung, dass der Hinweis auf das Widerspruchsrecht deutlich und getrennt von jeglicher anderer Information zu erfolgen hat. Für Unternehmen bedeutet dies in aller Regel eine Anpassung ihrer Datenschutzerklärungen.

g) Automatisierte Generierung von Einzelentscheidungen

Schließlich haben Betroffene das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkungen entfaltet, sofern nicht eine der normierten Ausnahmen greift.

4. Verantwortlichkeit und Auftragsdatenverarbeitung

Viele Regelungen der DSGVO sind deutschen Unternehmen bereits aus dem BDSG bekannt. Allerdings gibt es auch eine ganze Reihe von Veränderungen.

a) Gemeinsame Verantwortlichkeit

Neu ist die ausdrückliche Regelung, nach der mehrere Stellen gemeinsam für die Verarbeitung personenbezogener Daten verantwortlich sein können. Die DSGVO schreibt für diese Fälle vor, dass in einer Vereinbarung festgelegt werden muss, welche Stelle für welche Aufgaben nach der DSGVO verantwortlich ist. Betroffene haben unabhängig von der Aufgabenverteilung das Recht sich an jeden für die Verarbeitung Verantwortlichen zu wenden.

b) Verzeichnis der Verarbeitungstätigkeiten

Neben dem für die Verarbeitung Verantwortlichen hat zukünftig auch der Auftragsdatenverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Der Inhalt des Verzeichnisses entspricht im Wesentlichen den Anforderungen des BDSG an das Verfahrensverzeichnis, allerdings muss das Verzeichnis nach der DSGVO nicht mehr jedem Anfragenden, sondern nur noch der Aufsichtsbehörde auf Anforderung vorgelegt werden. Die Pflicht zur Führung eines solchen Verzeichnisses besteht nur, für Unternehmen oder Einrichtungen die 250 oder mehr Mitarbeiter beschäftigt, solange durch die Verarbeitung keine Risiken für Rechte und Freiheiten der Betroffenen bestehen. Bei der Verarbeitung sensibler Daten (z.B. Gesundheitsdaten) besteht die Pflicht immer.

c) Datenschutzfolgenabschätzung

Ähnlich der im BDSG geregelten Vorab-Kontrolle durch den betrieblichen Datenschutzbeauftragten verpflichtet die DSGVO die für die Verarbeitung Verantwortlichen zur Durchführung einer Datenschutzfolgeabschätzung, wen Verarbeitungen voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge haben. Die DSGVO nennt als Beispiele für solche Verfahren die systematische und umfassende Bewertung persönlicher Aspekte (z.B. Profiling), die umfangreiche Verarbeitung sensibler personenbezogener Daten oder die systematische weiträumige Überwachung öffentlich zugänglicher Bereiche. Die Aufsichtsbehörden können nach Abstimmung im Kohärenzverfahren Positiv- und Negativlisten veröffentlichen, für welche Verfahren Datenschutzfolgeabschätzungen durchzuführen sind und für welche nicht.

Ergibt sich aus einer Datenschutzfolgeabschätzung ein hohes Risiko und ergreift der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos ist die zuständige Aufsichtsbehörde zu konsultieren.

d) Vertreterbenennung durch Stellen außerhalb der EU

Sofern ein für die Verarbeitung Verantwortlicher oder ein Auftragsdatenverarbeiter selbst keine Niederlassung innerhalb der EU hat, ist er verpflichtet, einen Vertreter innerhalb der EU zu benennen, der für Betroffene und Aufsichtsbehörden als Anlaufstelle fungiert.

e) Technische und organisatorische Maßnahmen

Wie schon nach dem BDSG besteht auch nach der DSGVO eine Pflicht zur Einhaltung angemessener technischer und organisatorischer Maßnahmen. Die Struktur der Dokumentation der Maßnahmen wird sich durch die vom

BDSG abweichenden Kategorisierungen von Maßnahmen verändern, die Pflichten steigen aber für deutsche Unternehmen nicht wesentlich. Es dürfte sich allerdings anbieten, die veränderte Struktur bei der Überarbeitung und Neufassung von Dokumentationen bereits zu berücksichtigen, um den Aufwand bei Inkrafttreten der DSGVO überschaubar zu halten.

f) Privacy by Design

Die DSGVO verpflichtet den für die Verarbeitung Verantwortlichen dazu, bereits bei der Entwicklung von Produkten und Diensten datenschutzrechtliche Vorgaben wie die Datenminimierung zu berücksichtigen (z.B. Art und Umfang der erhobenen Daten, Pseudonomisierung und Anonymisierung, Zugriffsrechte und Speicherdauer). Ferner besteht die Verpflichtung, Standardeinstellungen so vorzunehmen, dass nur diejenigen Daten erhoben werden, den für den konkreten Zweck benötigt werden.

g) Auftragsdatenverarbeitung

Die Anforderungen und Vorgaben für Vereinbarungen zur Auftragsdatenverarbeitung (ADV) bleiben im Wesentlichen so, wie sie auch im BDSG geregelt sind. Erfreulich ist, dass die strenge deutsche Schriftform mit der DSGVO aufgehoben wird und eine ADV zukünftig auch elektronisch abgeschlossen werden kann. Neu ist, dass die EU Kommission Standardvertragsklauseln für die Auftragsdatenverarbeitung veröffentlichen kann und dass der Nachweis von Garantien des Auftragnehmers auch durch Zertifizierungen und genehmigte Verhaltensregeln (siehe unten Buchstabe j) erfolgen kann.

h) Datenschutzbeauftragter

Das Amt des betrieblichen Datenschutzbeauftragten wird durch die DSGVO europaweit eingeführt, allerdings nur für Unternehmen, deren Kerngeschäft Datenverarbeitungen sind, die besondere Risiken für den Betroffenen bergen, z.B. aufgrund einer umfangreichen und systematischen Beobachtung oder wegen der Verarbeitung besonders sensibler Daten. Wann genau eine Datenverarbeitung das Kerngeschäft eines Unternehmens darstellt und wann besondere Risiken vorliegen geht aus dem Text der DSGVO nicht klar hervor. Zudem wurde eine Öffnungsklausel aufgenommen, die es den Mitgliedsstaaten ermöglicht, die Bestellung eines Datenschutzbeauftragten auch in anderen Fällen verpflichtend zu machen. Es kann also durchaus sein, dass Deutschland die bestehende Bestellpflicht beibehalten wird.

i) Pflichten bei Datenschutzverstößen

Die DSGVO führt europaweit eine Pflicht zur Meldung von Datenschutzverletzungen ein, die den Regelungen des BDSG ähnelt. Neu ist, dass die Meldung an die Aufsichtsbehörde in der Regel innerhalb von höchstens 72 Stunden erfolgen muss. Die Pflicht zur Meldung entfällt jedoch, wenn durch die Verletzung keine Risiken für die Betroffenen entstehen. Unternehmen müssen außerdem jede Verletzung dokumentieren und Abhilfemaßnahmen treffen.

j) Verhaltensregeln und Zertifizierungen

Die DSGVO stellt erstmals umfassende Regelungen für die Einführung von Verhaltensregeln und Zertifizierungen auf. Danach können Verbände und Vereinigungen konkrete Verhaltensregeln im Zusammenhang mit der Datenverarbeitung für Ihre Mitglieder aufstellen und diese von den Aufsichtsbehörden freigeben lassen. Ziel dieser Regelungen soll es sein, gerade für kleinere

und mittlere Unternehmen einfache branchenübliche Vorgaben für den Datenschutz zu schaffen.

Die DSGVO regelt erstmals auch grundlegend die Anforderungen an Zertifizierungen. Solche können von unabhängigen Zertifizierungsstellen vergeben werden, die allerdings von den Aufsichtsbehörden akkreditiert werden müssen.

5. Übermittlungen in Drittländer und an internationale Organisationen

Der internationale Datentransfer wird in der DSGVO in einem eigenem Kapital geregelt. Damit wird die datenschutzrechtliche Bedeutung hervorgehoben und der internationale Datentransfer klar strukturiert. Dies ist lobenswert.

Aus den Erwägungsgründen ergibt sich, dass sich die Verhandlungsführer bei der Ausgestaltung des internationalen Datentransfers an den Grundsätzen des EuGH im Safe-Harbor-Urteil orientiert haben. So wird hervorgehoben, dass ein Drittland Garantien für ein angemessenes Schutzniveau bieten sollte, das im Wesentlichen dem innerhalb der Union gewährleisteten Schutzniveau gleichwertig ist. Die Garantien sollen insbesondere die Verfügbarkeit durchsetzbarer Rechte der Betroffenen, wirksame Rechtsbehelfe und die Möglichkeit der Geltendmachung von Schadensersatz sicherstellen. Es bleibt abzuwarten, inwiefern diese Punkte in der Praxis umgesetzt werden, insbesondere in Bezug auf die neue Vereinbarung zum Datentransfer zwischen der EU und den USA (EU-US Privacy Shield), welche derzeit von der Art.-29-Dateschutzgruppe geprüft wird.

In Bezug auf die Möglichkeiten den internationalen Datentransfer datenschutzrechtlich abzusichern, sieht die DSGVO wie bisher verschiedene Möglichkeiten vor: (i) Angemessenheitsbeschlüsse der Kommission, (ii) verbindliche unternehmensinterne Datenschutzvorschriften, (iii) Standarddatenschutzklauseln oder (iv) individuelle Vertragsklauseln. Neu in diesem Zusammenhang sind lediglich die detaillierte Aufzählung des Mindestinhalts für Binding Corporate Rules oder die Möglichkeit der nationalen Aufsichtsbehörden eigene Muster für Standarddatenschutzklauseln herauszugeben (welche jedoch von der Kommission genehmigt werden müssen). Ferner sind die Voraussetzungen für die Prüfung der Angemessenheit des gebotenen Schutzniveaus im Zusammenhang mit dem Angemessenheitsbeschluss der Kommission detailliert geregelt worden. Hier wurden ebenfalls die Grundsätze des Safe-Harbor-Urteils des EuGH berücksichtigt.

Aufgrund der Tatsache, dass zukünftig der Abstimmungsprozess unter den nationalen Aufsichtsbehörden gestrafft werden soll, steht zu erwarten, dass auch weltweit tätige mittelständische Unternehmen ihren internationalen Datenverkehr auf Binding Corporate Rules stützen können. Es entfällt sowohl zeitlicher als auch finanzieller Aufwand. Dies ist eine wesentliche Erleichterung im internationalen Datenverkehr.

Wie bislang schon der Fall, gibt es darüber hinaus geregelte Ausnahmefälle, in welchen eine Übermittlung auch ohne einen Angemessenheitsbeschluss der Kommission oder ausreichende Garantien beim Empfänger möglich ist. Die wichtigste Ausnahme in diesem Zusammenhang ist die Einwilligung des Betroffenen. Die Einwilligung muss in diesem Fall ausdrücklich erfolgen und der Betroffene muss über mögliche Risiken der Datenübermittlung aufgeklärt werden.

6. Aufsichtsbehörden

a) Nationale Aufsichtsbehörden

Die Mitgliedstaaten haben wie bisher für unabhängige Aufsichtsbehörden zu sorgen, die jedoch zur einheitlichen Anwendung der Verordnung mit der Kommission kooperieren müssen. In der Wahl ihrer Mitarbeiter sind die Aufsichtsbehörden frei und die Mitglieder der Aufsichtsbehörden sind weisungsfrei.

Mitarbeiter von Aufsichtsbehörden dürfen keine Tätigkeiten ausüben oder Ämter bekleiden, die mit der Aufgabe der Behörde nicht zu vereinbaren sind.

Wie schon nach geltendem deutschem Recht haben die Mitgliedstaaten für eine Ausstattung zu sorgen, die die effektive Aufgabenwahrnehmung ermöglicht. Auch die Finanzkontrolle darf die Unabhängigkeit nicht beeinträchtigen.

Aus mehreren nationalen Behörden wird jeweils ein Vertreter im „Europäischen Datenschutzausschuss“ bestimmt, der zukünftig ähnliche Aufgaben wahrnimmt, wie bisher die Art.-29-Datenschutzgruppe.

Die DSGVO enthält – auch als Ergebnis des Trilogs – einen sehr detaillierten Katalog sowohl zu den konkreten Aufgaben als auch den Befugnissen der Aufsichtsbehörden. Diese umfassen das Spektrum von Auskunftsrechten über Weisungen, Warnungen, Verbote und Bußgelder. Die Tätigkeit der Behörden ist wie bisher in einem Jahresbericht zusammenzufassen.

Die Zuständigkeit jeder Aufsichtsbehörde bleibt auf das Hoheitsgebiet des Mitgliedsstaates beschränkt. Grundsätzlich wird die nationale Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung der datenverarbeitenden Stelle als federführende Aufsichtsbehörde bestimmt, die bei grenzüberschreitenden Verarbeitungen zuständig ist.

b) Zusammenarbeit und Kohärenz

Die DSGVO enthält ein eigenes Kapitel, welches die Zusammenarbeit und Abstimmung der nationalen Aufsichtsbehörden regelt. Dadurch soll eine einheitliche Anwendung der DSGVO und damit mehr Rechtssicherheit erreicht werden. Es steht allerdings zu befürchten, dass der Abstimmungsprozess zu einer erheblichen Verlängerung der Verfahren führen wird.

Bei grenzüberschreitenden Sachverhalten hat die federführende Aufsichtsbehörde alle anderen involvierten Aufsichtsbehörden zu informieren und Entscheidungen vor Erlass mitzuteilen. Alle involvierten Aufsichtsbehörden dürfen dann eine Stellungnahme abgeben. Wird dabei ein begründeter erheblicher Einspruch eingelegt, wird die Sache dem Europäischen Datenschutzausschuss zur Streitbeilegung und Entscheidung vorgelegt: Erfolgt kein fristgerechter Einspruch durch eine involvierte nationale Aufsichtsbehörde oder hilft die federführende Aufsichtsbehörde dem Einspruch ab, wird die entsprechende Entscheidung der federführenden Aufsichtsbehörde für die anderen Aufsichtsbehörden bindend. Die federführende Aufsichtsbehörde kommuniziert die Entscheidung an die datenverarbeitende Stelle und die die auslösende Beschwerde empfangende nationale Aufsichtsbehörde an den Beschwerdeführer.

c) Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss ist für die Umsetzung und Überwachung des Datenschutzes zuständig. Er wird als unabhängiges Organ der Europäischen Union mit eigener Rechtspersönlichkeit etabliert und ist weisungsfrei. Ihm werden umfangreiche Aufgaben und Befugnisse zugewiesen,

die letztendlich die inhaltliche Herrschaft über die Interpretation der Datenschutzregeln beinhalten und ihm die Kompetenz über die Leitlinien zuweist.

Aufsichtsbehörden müssen vom Europäischen Datenschutzausschuss bei bestimmten Maßnahmen seine Stellungnahme einholen, unter anderem bei Fragen zu einem Verhaltenskodex, zu Standard Vertragsklauseln oder zu Binding Corporate Rules.

7. Rechtsbehelfe, Haftung und Sanktionen

Mit der DSGVO sollen die Betroffenenrechte gestärkt werden. Dazu werden dem Betroffenen bislang nicht vorhandene Instrumentarien zur Geltendmachung seiner Rechte zur Verfügung gestellt. Zugleich ermöglicht die DSGVO eine schärfere Sanktionierung von Datenschutzverstößen.

Besonders hervorzuheben ist die Einführung des Verbandsklagerechts für Datenschutzverstöße. Danach können insbesondere Verbraucherschutzverbände ein gerichtliches oder behördliches Verfahren wegen der Verletzung von Datenschutzvorschriften einleiten und führen. Das Verbandsklagerecht der DSGVO geht über das vom deutschen Gesetzgeber jüngst eingeführte Verbandsklagerecht bei Datenschutzverstößen hinaus. Neben den Aufsichtsbehörden werden zukünftig auch Verbände gegen jegliche Art von Datenschutzverstößen vorgehen können, etwa bei einer unrichtigen Datenschutzerklärung auf einer Webseite.

Verbände sind dabei auch zur Geltendmachung von Schadensersatzansprüchen Betroffener befugt, wenn sie von diesen damit beauftragt wurden. Nach der DSGVO können auch nicht-öffentliche Unternehmen dem Betroffenen gegenüber zum Ersatz immateriellen („moralischen“) Schadens verpflichtet sein. Der häufig schwierige Nachweis eines wirtschaftlichen Schadens ist zukünftig nicht mehr zwingend erforderlich. Außerdem kann nach der DSGVO neben der verantwortlichen Stelle auch der Auftragsdatenverarbeiter auf Schadensersatz haften.

Neben dieser erweiterten Haftung gegenüber den Betroffenen sieht die DSGVO für Datenschutzaufsichtsbehörden die Möglichkeit vor, bei Datenschutzverstößen erheblich höhere Bußgelder zu verhängen. Für Datenschutzverstöße drohen Bußgelder in Höhe von bis zu 10 Millionen Euro oder 4% des weltweit erzielten Gesamtumsatzes der Unternehmensgruppe.

Mit Inkrafttreten der DSGVO haben Unternehmen bei Datenschutzverstößen daher nicht nur mit durchsetzbaren Schadensersatzansprüchen Betroffener, sondern auch mit erheblich höheren Bußgeldern zu rechnen. Wegen des umfassenden Verbandsklagerechts ist zudem mit einem deutlich häufigeren behördlichen oder gerichtlichen Vorgehen bei Datenschutzverstößen zu rechnen.

8. Vorschriften für besondere Datenverarbeitungssituationen

Die DSGVO gibt zwar unmittelbar verbindliche Maßstäbe für den Datenschutz vor, enthält jedoch auch Öffnungsklauseln, die es den Mitgliedsstaaten ermöglichen, nationale Regelungen in bestimmten Bereichen zu treffen. Die ursprünglich von der EU-Kommission angestrebte Vollharmonisierung wird daher an mehreren Stellen durchbrochen.

a) Beschäftigtendaten

Der wohl für die meisten Unternehmen wichtigste Bereich, für den die DSGVO nicht abschließend ist, dürfte die Datenverarbeitung im Beschäftigungsverhältnis sein. Mitgliedstaaten können durch Gesetz oder Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen.

Beachtenswert ist hier, dass die DSGVO Kollektivvereinbarungen (Tarifverträge und Betriebsvereinbarungen) ausdrücklich erwähnt. Dies entspricht der bisherigen Rechtslage in Deutschland, wo insbesondere Betriebsvereinbarungen wichtige datenschutzrechtliche Gestaltungsinstrumente sind. Diskussionsstoff dürfte die Frage liefern, bis zu welchem Grad der Begriff „spezifischere Vorschriften“ den Mitgliedstaaten Abweichungen von den Vorgaben der DSGVO erlaubt.

Ob die DSGVO einen neuen Anschub für die Verabschiedung des seit Jahren geplanten Beschäftigtendatenschutzgesetzes in Deutschland gibt, ist wegen der nur allgemeinen Vorgaben in der DSGVO aber eher fraglich.

b) Verlage, Geheimnisträger, Kirchen

Erwähnenswert ist außerdem eine Öffnungsklausel bezogen auf Meinungsäußerung und Informationsfreiheit, die mittelbar z.B. die Verlagsbranche betreffen könnte. Träger von Berufsgeheimnissen könnten zudem entsprechend von der Öffnungsklausel im Bereich Geheimhaltungspflichten betroffen sein. Auch kirchliche Sonderregelungen zum Datenschutz können unter bestimmten Voraussetzungen Vorrang vor den Bestimmungen der DSGVO genießen.

Die jeweiligen nationalen Entwicklungen in diesen datenschutzsensiblen Bereichen bleiben abzuwarten und sollten beobachtet werden.

9. Delegierte Rechtsakte und Durchführungsakte

Die EU-Kommission erhält zukünftig das Recht sog. delegierte Rechtsakte zur DSGVO zu erlassen. Dabei handelt es sich um Ausführungsbestimmungen zu einzelnen Vorschriften der DSGVO, die den Erlass eines delegierten Rechtsakts vorsehen. Beispiele sind Darstellung von Informationen für die betroffenen Personen durch Bildsymbole oder Anforderungen an datenschutzspezifische Zertifizierungsverfahren. Darüber hinaus soll die EU-Kommission von einem Ausschuss unterstützt werden.

10. Schlussbestimmungen

Internationale Übereinkünfte, die die Weitergabe personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, bleiben bestehen, wenn sie vor Inkrafttreten dieser Verordnung geschlossen wurden. Unter besonderer Beobachtung und wiederkehrender Überprüfung bleiben u.a. die Übertragung von Daten in Drittländer oder an internationale Organisationen sowie der Europäische Datenschutzausschuss und die Zusammenarbeit der Staaten.