

DSG-Info-Service

Juni 2015

Ausgabe Nr. 78-80

*Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!*

Nach über drei Jahren andauernden zähen Verhandlungen, haben sich die Innen- und Justizminister am 15. Juni 2015 endlich auf eine gemeinsame Position zur geplanten DS-GVO

geeignet (<http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf>). Die vorliegende Information gibt den derzeitigen Verhandlungsstand in Bezug auf einige wichtige Bestimmungen für die österreichische Wirtschaft wieder, bei Notwendigkeit ergänzt um entsprechende Anmerkungen.

1. Einleitung

In den Ausgaben Nr. 74 – 77 haben wir Sie jeweils über die Zwischenergebnisse bei den Verhandlungen über die Gestaltung der DS-GVO informiert. Nunmehr ist man in Brüssel einen wesentlichen Schritt weitergekommen: Es war eine schwere Geburt, bis sich die Innen- und Justizminister der EU-Mitgliedstaaten auf eine gemeinsame Linie zur geplanten DS-GVO geeinigt haben, wobei Österreich, vertreten durch den Justizminister Dr. Brandstetter gegen diesen Kompromiss stimmte. Dies mit der Begründung, dass die Position der Justizminister hinter dem heutigen Schutzstandard in Österreich und auch hinter den Mindeststandards der EU zurückbleiben würden. Auch andere Minister äußerten schwere Bedenken gegen den Kompromisstext, stimmten aber dem Mandat für die Aufnahme der Verhandlungen mit dem EU-Parlament und der Kommission dennoch zu.

Nun kann die Lobby Schlacht beginnen, oder besser gesagt fortgesetzt werden, denn Par-

lament, Kommission und Rat müssen sich im sogenannten Trilog auf ein gemeinsames Papier einigen. Die entsprechenden Verhandlungen zwischen Ministern, EU-Abgeordneten und der EU-Kommission sollen bereits am 24. Juni beginnen und mit Ende 2015 abgeschlossen sein. Somit könnte – wenn dieser ambitionierte Zeitplan hält – die DS-GVO in allen 28 EU-Mitgliedstaaten mit 1. Jänner 2018 in Kraft treten. Die diversen Medienausagen von Jan Philipp Albrecht, Berichterstatter des Europäischen Parlaments für die Reform der DS-GVO und grüner EU-Abgeordneter, über das seines Erachtens derzeit noch bestehende große Auseinanderklaffen zwischen Verbraucherrechten und Unternehmenspflichten, lassen allerdings befürchten, dass der Trilog noch länger dauern könnte.

Nichts desto trotz sollte man sich mit einigen wichtigen Punkten des Entwurfs schon jetzt auseinandersetzen.

2. DS-GVO – Ausgewählte Bestimmungen

Artikel 4, Abs. 1 **Begriffsbestimmungen**

Im Sinne dieser Verordnung bezeichnet der Ausdruck

(1) „personenbezogene Daten“ alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person („betroffene Person“) beziehen; als bestimmbar wird eine Person angesehen, die direkt oder indirekt (...), insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen bestimmt werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

Anmerkung: Wie bereits aus Art. 1, Abs. 1 und 2 hervorgeht, gilt die DS-GVO nur für **natürliche Personen** und nicht für **juristische Personen**, so wie es derzeit das österreichische DSG 2000 noch vorsieht, und zwar dann, wenn das Grundrecht zur Anwendung kommen kann, wobei der VfGH in seiner ständigen Judikatur davon ausgeht, dass Wirtschaftsdaten personenbezogene Daten eines Betroffenen sein können. Art. 4 Abs. 1 DS-GVO stellt klar, dass sich personenbezogene Daten nur auf natürliche Personen beziehen können.

Nach Erwägungsgrund 24 der RL 95/46/EG (Anm: Präambeln in Form der Erwägungsgründe (EG), die den europäischen Rechtsakten, insbesondere den Richtlinien, vorangestellt sind, geben Hinweise auf die authentische Auslegung des Rechtsakts, also die Auslegung, die der Normgeber beachtet wissen will. EG entsprechen etwas den Erläuterungen zu Regierungsvorlagen bzw. den Ausschussberichten zu österreichischen Gesetzen) berührt die RL nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten. Somit ist es den EU-MS – wie Öster-

reich, Dänemark und Luxemburg - freigestanden, den Schutz der personenbezogenen Daten im Rahmen des jeweiligen nationalen Datenschutzrechts auf juristische Personen auszudehnen.

Alle Interventionen der österreichischen Wirtschaftsvertreter in Brüssel in der DS-GVO auch den Schutz der Daten juristischer Personen vorzusehen, haben nichts genützt! Die Daten der juristischen Personen sind in der DS-GVO kein „Schutzobjekt“. Wie wir bereits in unserer Ausgabe Nr. 74 ausführten, stellt diese Bestimmung eine Ungleichbehandlung zwischen Kapitalgesellschaften (AG, GmbH) und Einzelunternehmen (EPU) dar, da die gewerblichen Schutzrechte bzw. Urheberrechte nur dann den Schutz von Geschäfts- und Betriebsgeheimnissen bieten, wenn entsprechende Schutzrechte beantragt wurden und etwa ein Patent angemeldet ist (Formalschutz). Der Anwendungsbereich der Wirtschaftsdaten ist in der Praxis wesentlich weiter und daher ist aus Sicht der österreichischen Wirtschaft die Beibehaltung des Datenschutzes auch für die juristischen Personen notwendig.

Artikel 4, Abs. 8

Im Sinne dieser Verordnung bezeichnet der Ausdruck

...

(8) „Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene (...) Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Anmerkung: Die noch im Kommissionsentwurf vom 25. Jänner 2012 geforderte „explizite“ Willensbekundung wurde im Kompromisspaket vom 12. März 2014 in „ausdrückliche“ so-

wie am Ende der italienischen Präsidentschaft auf „unzweideutig“ geändert. Mit diesen Wortspielereien ist derzeit Schluss! Mit der derzeitigen Formulierung könnte die Wirtschaft gut leben, wäre da nicht der EG 34, der wie folgt lautet:

„Um sicherzustellen, dass die Einwilligung ohne Zwang erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung ohne Zwang gegeben wurde, keine rechtliche Handhabe liefern. Die Einwilligung gilt nicht als ohne Zwang erteilt, wenn zu verschiedenen Datenverarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird, obwohl dies für diese Erfüllung nicht erforderlich ist, und der betroffenen Person ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht in zumutbarer Weise möglich ist.“

Damit ist offensichtlich jenes, mit der Ungleichgewichtung der Partner – Betroffener und Auftraggeber – zusammenhängende Gültigkeitsproblem einer Zustimmungserklärung in den EG 34 gewandert. Damit stellt dieser EG eine ernste Gefahr für einen sicheren Rechts- und Geschäftsverkehr dar.

Artikel 6

Rechtmäßigkeit der Verarbeitung

1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

(a) Die betroffene Person hat ihre unmissverständliche Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben;

(b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene

Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;

(c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

(d) die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen;

(e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

(f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. (...).

2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke oder für historische, statistische oder wissenschaftliche Zwecke unterliegt auch den Bedingungen und Garantien des Artikels 83.

3. Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e muss festgelegt werden im Einklang mit

(a) dem Unionsrecht oder

(b) dem nationalen Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der

Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Datenverarbeitung durch den für die Verarbeitung Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die Daten weitergegeben werden dürfen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer Verarbeitung nach Recht und Gesetz, unter anderem für sonstige spezifische Verarbeitungssituationen gemäß Kapitel IX.

3a. Um sich in Fällen, in denen die betroffene Person keine Einwilligung erteilt hat, zu vergewissern, ob ein Zweck der Weiterverarbeitung (...) mit demjenigen vereinbar ist, zu dem die Daten ursprünglich erhoben wurden, berücksichtigt der für die Verarbeitung Verantwortliche unter anderem

(a) jede Verbindung zwischen den Zwecken, für die die Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

(b) den Zusammenhang, in dem die Daten erhoben wurden,

(c) die Art der personenbezogenen Daten, insbesondere ob besondere Datenkategorien gemäß Artikel 9 verarbeitet werden,

(d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

(e) das Vorhandensein angemessener Garantien.

4. Wenn der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten von demselben für die Verarbeitung Verantwortlichen erhoben wurden, nicht vereinbar ist, muss auf die Weiterverarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Die Weiterverarbeitung durch denselben für die Verarbeitung Verantwortlichen für nicht konforme

Zwecke aufgrund der berechtigten Interessen dieses für die Verarbeitung Verantwortlichen oder eines Dritten ist rechtmäßig, wenn diese Interessen die Interessen der betroffenen Person überwiegen.

5. (...)

Anmerkung: Unter den europäischen Datenschützern sind besonders die Abs. 3a und 4 stark umstritten. Die Liste in Abs. 3a definiert nämlich, unter welchen Umständen Daten für andere Zwecke – ohne Einwilligung des Betroffenen – verarbeitet werden dürfen, als für den, für den sie erhoben wurden.

Nach den derzeitigen Bestimmungen des Abs. 4 können personenbezogene Daten auch dann für andere Zwecke als ursprünglich vorgesehen verarbeitet werden, wenn der Auftraggeber oder ein Dritter daran ein „berechtigtes Interesse“ (Abs. 1 lit. f) hat, das schwerer wiegt als jenes des Betroffenen. Das heißt, der Zweck der personenbezogenen Datenerhebung kann also im Nachhinein geändert werden, wenn ein anderer Grund wie in Abs. 1 lit. a) bis e) angegeben, dies rechtfertigt. Dies können vertragliche Verpflichtungen, Einwilligungen oder öffentliches Interesse oder lebenswichtige Interessen der Betroffenen sein.

Ganz zu verstehen ist die Aufregung unter den Datenschützern nach Ansicht des Verfassers nicht, weil zB auch das DSG 2000 schon derzeit in den Bestimmungen der §§ 8 und 9 die Möglichkeit offen lässt, vom Grundsatz der Zweckbindung zur Wahrung berechtigter Interessen eines Dritten abzuweichen. Dies entspricht der Regelung, die der Rat nunmehr im Rahmen der DS-GVO fordert. Aus Sicht der Wirtschaft ist die derzeitige Formulierung als positiv zu werten.

Artikel 7

Bedingungen für die Einwilligung

1. In den Fällen, in denen Artikel 6 Absatz 1 Buchstabe a zur Anwendung kommt, muss der für die Verarbeitung Verantwortliche nachwei-

sen können, dass die betroffene Person ihre unmissverständliche Einwilligung erteilt hat.

1a. In den Fällen, in denen Artikel 9 Absatz 2 Buchstabe a zur Anwendung kommt, muss der für die Verarbeitung Verantwortliche nachweisen können, dass die betroffene Person ihre ausdrückliche Einwilligung erteilt hat.

2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es (...) von den anderen Sachverhalten klar zu unterscheiden ist.

3. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt.

4. (...)

Anmerkung: Gem. Abs. 1 wird der Auftraggeber nach der allgemeinen Beweislastregel die Beweislast tragen müssen. Es ist demzufolge seine Aufgabe, die Einwilligung zur Absicherung in geeigneter Form zu dokumentieren. Diese Aufgabe trifft sowohl auf die in Abs. 1 enthaltene „einfache“ Zustimmung wie auch auf die in Abs. 1a „ausdrückliche“ Zustimmung zu. Diese Beweislastregel, wonach immer automatisch der Auftraggeber die unzweifelhafteste Zustimmung zu beweisen hat, ist aus Sicht der Wirtschaft mehr als unangenehm, und läuft dem Prinzip der prozessualen Waffengleichheit zuwider. Grundsätzlich sollte nach Ansicht des Verfassers, jede Partei – Auftraggeber und Betroffener – ihre Behauptungen zwecks Darstellung ihrer Ansprüche beweisen und darlegen.

Abs. 2 wirft generell die Frage auf, ob eine Offline-Zustimmung und eine Online-Zustimmung gleich zu behandeln sind.

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

1. Der für die Verarbeitung Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 14 und 14a und alle Mitteilungen gemäß den Artikeln 15 bis 19 und Artikel 32, die sich auf die Verarbeitung personenbezogener Daten beziehen, in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls in elektronischer Form. Stellt die betroffene Person den Antrag in elektronischer Form, so kann sie in der Regel auf elektronischem Weg unterrichtet werden, sofern sie nichts anderes angibt. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person nachgewiesen ist.

1a. Der für die Verarbeitung Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 19. In den in Artikel 10 Absatz 2 genannten Fällen kann sich der für die Verarbeitung Verantwortliche nur weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 19 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu bestimmen.

2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person Informationen über auf Antrag gemäß den Artikeln 15 und 16 bis 19 ergriffene Maßnahmen ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Antrags zur Verfügung (...). Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität des Antrags und der Anzahl von Anträgen erforderlich ist. Kommt es zu einer Fristverlängerung, so wird die betroffene Person innerhalb

eines Monats nach Eingang des Antrags über die Gründe für die Verzögerung informiert.

3. Wird der für die Verarbeitung Verantwortliche auf Antrag der betroffenen Person nicht tätig, so unterrichtet er die betroffene Person ohne ungebührliche Verzögerung und spätestens innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen (...).

4. Informationen gemäß den Artikeln 14 und 14a (...) und alle Mitteilungen gemäß den Artikeln 16 bis 19 und Artikel 32 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall ihrer Häufung – unverhältnismäßigen Anträgen einer betroffenen Person kann sich der für die Verarbeitung Verantwortliche weigern, aufgrund des Antrags tätig zu werden (...). In diesem Fall hat er den Nachweis für den offenkundig unbegründeten oder unverhältnismäßigen Charakter des Antrags zu erbringen.

4a. Hat der für die Verarbeitung Verantwortliche begründete Zweifel an der Identität der Person, die den Antrag gemäß den Artikeln 15 bis 19 stellt, so kann er unbeschadet des Artikels 10 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

5. (...)

6. (...)

Anmerkung: Abs. 2 verkürzt die derzeit in § 26 Abs. 4 DSG 2000 enthaltene Auskunftsfrist von 8 Wochen auf 1 Monat. Diese Verkürzung könnte in der Praxis Probleme mit sich bringen.

ABSCHNITT 2

INFORMATIONSPFLICHT UND AUSKUNFTS- RECHT

Artikel 14

Informationspflicht bei Erhebung der Daten bei der betroffenen Person

1. Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen

Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

(a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters; zusätzlich werden, falls vorhanden, auch die Kontaktdaten des Datenschutzbeauftragten angegeben;

(b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden, (...) sowie die Rechtsgrundlage für die Verarbeitung.

1a. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung der personenbezogenen Daten folgende weitere Informationen zur Verfügung, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um (...) eine faire und transparente Verarbeitung zu gewährleisten:

(a) (...);

(b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt werden;

(c) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

(d) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, personenbezogene Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln;

(e) das Bestehen eines Rechts auf Auskunft seitens des für die Verarbeitung Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung dieser Daten und eines Widerspruchsrechts gegen die Verarbeitung dieser Daten (...) sowie des Rechts auf Datenübertragbarkeit;

(ea) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines

Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

(f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...);

(g) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte;

(h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und Angaben zu (...) der verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

1b. Beabsichtigt der für die Verarbeitung Verantwortliche, die Daten (...) für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen relevanten Informationen gemäß Absatz 1a zur Verfügung.

2. (...)

3. (...)

4. (...)

5. Die Absätze 1, 1a und 1b finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

6. (...)

7. (...)

8. (...)

Anmerkung: Überbordend ist in Bezug auf die Informationspflicht die Bestimmung des Art. 14 Abs. 1a, die besagt, dass der Auftraggeber, unabhängig von einer konkreten Nachfrage des Betroffenen, die in den lit. b) bis h) angeführten Informationen erteilen soll. Aus Sicht der Wirtschaft wäre es wünschenswert,

dass diese Informationspflicht eine konkrete Nachfrage des Betroffenen voraussetzt.

Artikel 14a

Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden

1. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen Person Folgendes mit:

(a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters; zusätzlich werden, falls vorhanden, auch die Kontaktdaten des Datenschutzbeauftragten angegeben;

(b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung.

2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person folgende weitere Informationen zur Verfügung, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

(a) die Kategorien personenbezogener Daten, die verarbeitet werden;

(b) (...)

(c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt werden;

(d) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

(da) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, personenbezogene Daten an einen Empfänger in einem Drittland oder eine internationale Organisation zu übermitteln;

(e) das Bestehen eines Rechts auf Auskunft seitens des für die Verarbeitung Verantwortli-

chen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung dieser Daten und eines Widerspruchsrechts gegen die Verarbeitung dieser Daten sowie des Rechts auf Datenübertragbarkeit (...);

(ea) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

(f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...);

(g) aus welcher Quelle die [...] personenbezogenen Daten stammen, sofern diese nicht aus öffentlich zugänglichen Quellen stammen;

(h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und Angaben zu der verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

3. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

(a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der Daten innerhalb einer angemessenen Frist nach Erhebung der Daten, längstens jedoch innerhalb eines Monats, oder,

(b) falls die Weitergabe an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.

3a Beabsichtigt der für die Verarbeitung Verantwortliche, die Daten (...) für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen relevanten Informationen gemäß Absatz 2 zur Verfügung.

4. Die Absätze 1 bis 3a finden keine Anwendung, wenn und soweit

(a) die betroffene Person bereits über die Informationen verfügt oder

(b) die Erteilung dieser Informationen (...) sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; in diesen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person; oder

(c) die Erhebung oder Weitergabe durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

(d) (...);

(e) die Daten gemäß dem Unionsrecht oder dem einzelstaatlichen Recht (...) vertraulich behandelt werden müssen.

5. (...)

6. (...)

Anmerkung: Siehe Anmerkung zu Art. 14, die auch auf Abs. 2 des Art. 14a zutrifft.

Artikel 15

Auskunftsrecht der betroffenen Person

1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen in angemessenen Abständen unentgeltlich (...) eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese Daten und auf folgende Informationen:

(a) die Verarbeitungszwecke;

(b) (...)

(c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in

Drittländern oder bei internationalen Organisationen;

(d) wenn möglich, die geplante Speicherfrist;

(e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung dieser Daten durch den für die Verarbeitung Verantwortlichen oder eines Widerspruchsrechts gegen die Verarbeitung dieser Daten;

(f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (...);

(g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

(h) im Fall von Entscheidungen, die auf einer automatisierten Verarbeitung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 beruhen, Angaben zu der verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung.

1a. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 42 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

1b. Auf Antrag stellt der für die Verarbeitung Verantwortliche der betroffenen Person, ohne eine überhöhte Gebühr zu verlangen, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

2. (...)

2a. Der Anspruch auf eine Kopie gemäß Absatz 1b (...) besteht nicht, wenn eine solche nicht zur Verfügung gestellt werden kann, ohne personenbezogene Daten anderer betroffener Personen oder vertrauliche Daten des für die Verarbeitung Verantwortlichen offenzulegen. Ferner besteht dieser Anspruch nicht, wenn die Offenlegung personenbezogener Daten Rechte an geistigem Eigentum in Bezug auf die Verarbeitung dieser personenbezogenen Daten verletzen würde.

3. (...)

4. (...)

Anmerkung: Dieser Artikel ist nach Meinung des Verfassers mehr als entbehrlich, da hier eine weitgehende Überlappung mit den Bestimmungen der Art. 12 bis 14a festzustellen ist.

Artikel 17

Recht auf Löschung und auf „Vergessenwerden“

1. (...) Der für die Verarbeitung Verantwortliche ist verpflichtet, personenbezogene Daten ohne ungebührliche Verzögerung zu löschen, insbesondere personenbezogene Daten, die erhoben wurden, als die betroffene Person ein Kind war, und die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten ohne ungebührliche Verzögerung gelöscht werden, sofern einer der folgenden Gründe zutrifft:

(a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

(b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, (...) und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.

(c) Die betroffene Person legt gemäß Artikel 19 Absatz 1 Widerspruch gegen die Verarbeitung personenbezogener Daten ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 19 Absatz 2 Widerspruch gegen die Verarbeitung ein.

(d) Die Daten wurden unrechtmäßig verarbeitet.

(e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.

1a. Die betroffene Person hat ferner das Recht, von dem für die Verarbeitung Verantwortlichen

chen die Löschung sie betreffender personenbezogener Daten ohne ungebührliche Verzögerung zu verlangen, wenn die Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben wurden.

(...).

2. (...).

2a. Hat der (...) für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so unternimmt er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten (...) vertretbare Schritte, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.

3. Die Absätze 1, 1a und 2a gelten nicht, soweit (...) die Verarbeitung der personenbezogenen Daten erforderlich ist

a. zur Ausübung des Rechts auf freie Meinungsäußerung und Information ;

b. zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung personenbezogener Daten nach dem Unionsrecht oder dem einzelstaatlichen Recht, dem der für die Verarbeitung Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

c. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und hb sowie Artikel 9 Absatz 4;

d. für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche, statistische und historische Zwecke gemäß Artikel 83;

e. (...)

f. (...)

g. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

4. (...)

5. (...)

Anmerkung: Dieser Artikel enthält das Löschen von Daten und präzisiert diesen Anspruch des Betroffenen auf ein Recht auf „Vergessenwerden“. Abs. 2a enthält verschärfte Anforderungen und daraus abzuleitende Handlungspflichten, wenn der Auftraggeber die Daten veröffentlicht hat. Gemeint ist hier die Veröffentlichung durch das Internet. In diesem Fall muss der Auftraggeber alle vertretbaren Schritte unternehmen, auch technischer Art, um weitere Auftraggeber, die diese Daten verarbeiten, darüber zu informieren, dass ein Betroffener die Löschung aller Querverweise gefordert hat. Die ursprünglich geplante Pflicht des Auftraggebers selbst für die Löschung der Links und Kopien bezüglich der in Frage stehenden Daten zu sorgen, wurde vernünftigerweise durch die Formulierung „vertretbare Schritte“ gemildert. Dies deshalb, weil sich bekanntlich Inhalte im Internet in kürzester Zeit vervielfältigen und eine Löschung dieser Daten eine kaum zu bewältigende Aufgabe darstellen würde. Insgesamt ist dieser Artikel aber unausgegoren und schafft für die Unternehmen keine rechtssichere Regelung.

Artikel 18

Recht auf Datenübertragbarkeit

1. (...)

2. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen ohne Behinderung durch den für die Verarbeitung Verantwortlichen, dem die Daten bereitgestellt wurden, zu übermitteln, sofern

die Verarbeitung auf einer Zustimmung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

die Verarbeitung mit automatischen Mitteln erfolgt.

2a. Die Ausübung dieses Rechts lässt Artikel 17 unberührt. Das Recht gemäß Absatz 2 gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde.

2aa. Das Recht gemäß Absatz 2 gilt nicht, wenn die Offenlegung personenbezogener Daten die Rechte an geistigem Eigentum im Zusammenhang mit der Verarbeitung dieser personenbezogenen Daten verletzen würde.

3. (...)

4. (...).

Anmerkung: Das Recht auf Datenübertragbarkeit in einem strukturierten, gängigen und maschinenlesbaren Format ist auf Informationen beschränkt, die der Betroffene selbst zur Verfügung gestellt hat. Die Regelung bezieht sich offensichtlich auf die Anbieter sozialer Netzwerke, obgleich der Anwendungsbereich dieser geplanten Regelung nicht auf diese beschränkt ist.

Artikel 28

Aufzeichnungen zu den Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten

1. Alle für die Verarbeitung Verantwortlichen (...) und gegebenenfalls ihre Vertreter führen eine Aufzeichnung zu allen Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten, die ihrer Zuständigkeit unterliegen. Diese Aufzeichnung enthält folgende Angaben:

(a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen und etwaiger gemeinsam mit ihm Verantwortlicher (...), des

Vertreters des für die Verarbeitung Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

(b) (...)

(c) Angaben über die Zwecke der Verarbeitung einschließlich des berechtigten Interesses, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet;

(d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;

(e) die (...) Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern;

(f) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation (...);

(g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien.

(h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.

2a. Jeder Auftragsverarbeiter führt eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten, die Folgendes enthält:

(a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes für die Verarbeitung Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Vertreters des für die Verarbeitung Verantwortlichen;

(b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;

(c) die Kategorien der Verarbeitungen, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden;

(d) gegebenenfalls die Kategorien der Übermittlungen personenbezogener Daten an ein

Drittland oder an eine internationale Organisation.

(e) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 30 Absatz 1.

3a. Die in den Absätzen 1 und 2a genannten Aufzeichnungen sind schriftlich zu führen; dies schließt elektronische oder andere ohne technische Vermittlung nicht lesbare Formate, die in ein lesbares Format umgewandelt werden können, ein.

3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen der Aufsichtsbehörde die Aufzeichnung (...) auf Anforderung zur Verfügung.

4. Die in den Absätzen 1 und 2a genannten Pflichten gelten nicht für:

(a) (...);

(b) Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht aufgrund ihrer Art, ihres Umfangs, ihrer Umstände oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, unbefugte Umkehr der Pseudonymisierung, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile für die betroffenen Personen.

5. (...)

6. (...)

Anmerkung: Die in diesem Artikel vorgeschriebene durch den Auftraggeber zu führende Dokumentation über die einzelnen Datenanwendungen entspricht inhaltlich in etwa den in § 19 DSG 2000 angeführten Meldeunterlagen. Neu ist hingegen die Regelung gem. Abs. 2a, dass auch der Dienstleister entsprechende Aufzeichnungen zu führen hat.

ABSCHNITT 3

DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION

Artikel 33

Datenschutz-Folgenabschätzung

1. Wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, wie etwa Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, unbefugte Umkehr der Pseudonymisierung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, so führt der für die Verarbeitung Verantwortliche (...) vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (...).

1a. Der für die Verarbeitung Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

2. Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

(a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, (...) die sich auf Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber betroffenen Personen entfalten oder erhebliche Auswirkungen für diese mit sich bringen;

(b) Verarbeitung spezieller Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 (...), biometrischen Daten oder Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen, wenn die Daten in großem Umfang im Hinblick auf Entscheidungen verarbeitet werden, die sich auf spezifische Einzelpersonen beziehen sollen;

(c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen (...);

(d) (...);

(e) (...).

2a. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss.

2b. Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Europäischen Datenschutzausschuss.

2c. Vor Festlegung der in den Absätzen 2a und 2b genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 57 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

3. Die Folgenabschätzung enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung des Risikos, auf das in Absatz 1 Bezug genommen wird, sowie der geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

3a. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 38 durch die zuständigen für die Verarbeitung Verantwortlichen oder die

zuständigen Auftragsverarbeiter ist bei der Beurteilung der Rechtmäßigkeit und der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgängen, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

4. Der für die Verarbeitung Verantwortliche holt den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge (...) ein.

5. Falls (...) die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, beruht und falls die betreffenden Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln, gelten die Absätze 1 bis 3 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

6. (...)

7. (...)

Anmerkung: Gem. Art. 33 Abs. 1 DS-GVO muss der Auftraggeber vor Aufnahme einer Datenanwendung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung, voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten hat, vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen. Im Prinzip stellt diese Forderung eine Verlagerung der in Österreich gem. § 18 Abs. 2 vorgesehenen und von der DSB durchgeführten Vorabkontrolle für Datenanwendungen, die sensible Daten enthalten oder strafrechtlich relevante iSd § 8 Abs. 4 DSG 2000 oder die Auskunftserteilung über die Kreditwürdigkeit des Betroffenen zum Zweck haben bzw. in Form eines Informationsverbundsystems durchgeführt werden, zum Auftraggeber dar.

Konkrete Beispiele, in welchen Fällen in Zukunft eine Datenschutz-Folgenabschätzung vorzunehmen sein wird, sind zB Projekte, bei welchen die RFID-Technik eingesetzt wird oder die als Big Data-Projekte eingestuft werden können bzw. wenn es sich um solche Datenanwendungen handelt, die in Kapitel IX der DS-GVO angeführt sind, wie die Verarbeitung personenbezogener Daten für Gesundheitszwecke (Art. 81) oder die Verarbeitung genetischer Daten (Art. 81a). Weiters ist gem. Abs. 2 eine Datenschutz-Folgenabschätzung auch dann erforderlich, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durchgeführt wird („Profiling“), biometrische Daten verwendet werden oder Videoüberwachung eingesetzt wird.

Gem. Art. 4 der DS-GVO werden diese besonders sensiblen Daten wie folgt definiert:

(10) „genetische Daten“ personenbezogene Daten jedweder Art zu den (...) ererbten oder erworbenen genetischen Merkmalen eines Menschen, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden;

(11) „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die die eindeutige Identifizierung dieses Menschen ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

(12) „Gesundheitsdaten“ Daten, die sich auf die körperliche oder geistige Gesundheit einer Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

(12a) „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten,

insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren und vorherzusagen;

Gem. Abs. 1a berät der DSB – falls ein solcher ernannt sein sollte – den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung.

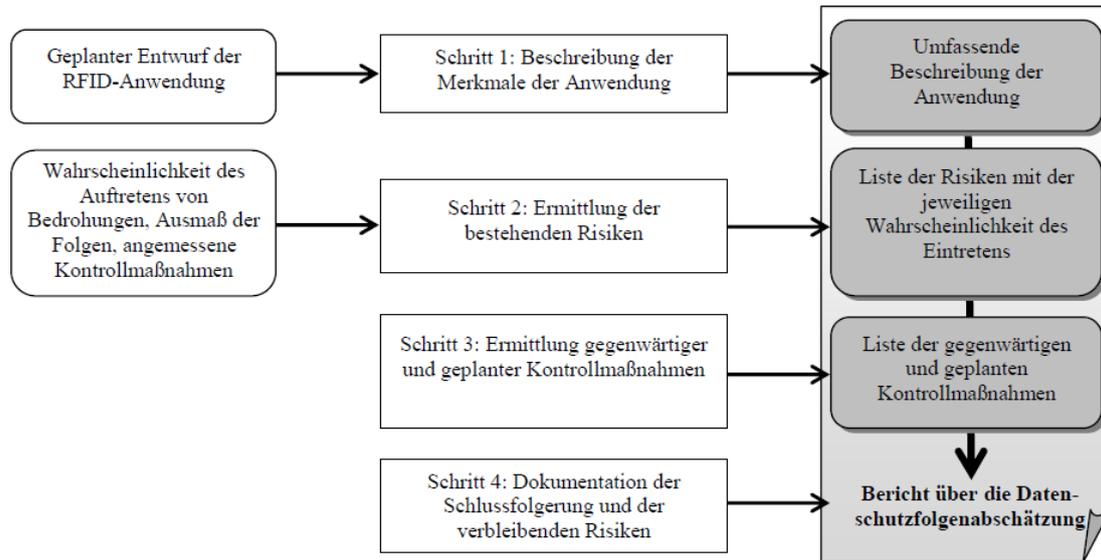
Entsprechend den Bestimmungen des Abs. 2a erstellt die nationale Aufsichtsbehörde eine Liste, die jene Datenanwendungen enthält, für die eine Datenschutz-Folgenabschätzung vorzunehmen ist (Positivliste) bzw. kann sie gem. Abs. 2b auch eine Liste über jene Datenanwendungen erstellen, für die keine Datenschutz-Folgenabschätzung angestellt werden muss (Negativliste). Als Beispiel für die Umsetzung dieser Forderungen könnte nach Ansicht des Verfassers die derzeit im DSG 2000 in der Standard- und Musterverordnung 2004 (StMV 2004) angeführten Standard- und Musteranwendungen herangezogen werden. Beide Listen sind in Form eines Beschlussentwurfes von der nationalen Aufsichtsbehörde an den Europäischen Datenschutzausschuss zur Einleitung des in Art. 57 DS-GVO vorgesehenen Kohärenzverfahrens zu übermitteln. Gem. Art. 58 DS-GVO übermittelt der Europäische Datenschutzausschuss den Beschlussentwurf an seine Mitglieder zur Prüfung. Erheben diese innerhalb einer vom Europäischen Datenschutzausschuss festgelegten Frist keine Einwände, dann gilt der Beschlussentwurf als angenommen.

Durch das Kohärenzverfahren soll gem. EG 103 eine einheitliche Anwendung und Durchsetzung der DS-GVO im Binnenmarkt gewährleistet werden.

Die in Abs. 3 DS-GVO enthaltene Kurzbeschreibung des Inhalts einer Datenschutz-Folgenabschätzung kann beispielsweise anhand des Dokuments „Rahmen für die Folgen-

abschätzung in Bezug auf den Datenschutz und die Wahrung der Privatsphäre bei RFID-Anwendungen“ (http://www.bfdi.bund.de/SharedDocs/Publikationen/RFID_PIA.de.html) vom 11. Februar 2011 wie folgt grafisch dar-

gestellt werden. Dieses Dokument setzt sich zwar mit einem speziellen Datenschutzthema auseinander, nämlich dem Einsatz von RFID, hat aber auch durchaus für andere Datenanwendungen Geltung:



Die einzelnen Schritte umfassen folgende Aktivitäten:

Schritt 1: Beschreibung der Merkmale der Anwendung

In dieser Phase ist die Anwendung, für die eine Datenschutz-Folgenabschätzung durchgeführt werden soll, möglichst umfassend zu beschreiben (Zweck der Datenanwendung, Betroffenenkreise, Datenarten mit Angaben über ihre Sensibilität, Übermittlungsempfänger nach EWR- und Drittstaaten, Dauer der Speicherung, Löschfristen). Ziel dieser Beschreibung ist es, ein möglichst umfassendes und vollständiges Bild der Datenanwendung zu erhalten.

Schritt 2: Ermittlung der Risiken

In dieser Phase ist eine Risikoanalyse durchzuführen. Diese beginnt mit der Ermittlung jener potenziellen Risiken der Datenanwendung, welche die Einhaltung der in der DS-GVO enthaltenen Zielen entgegenstehen (Gewährleistung der Datenqualität, Rechtmäßigkeit der

Verarbeitung, Einhaltung der Informationsverpflichtungen sowie des Auskunfts-, Richtigstellungs- und Löschungsrechts, Einhaltung des Widerspruchsrechts, Beachtung der Sicherheit der Verarbeitung, Einhaltung der Meldeanforderungen etc.).

Nach Ermittlung der potenziellen Risiken sind aus Sicht des Datenschutzes folgende Beurteilungen vorzunehmen:

1. Risikohöhe und Eintrittswahrscheinlichkeit
2. Ausmaß der Folgen bei Eintritt des Risikos

Schritt 3: Ermittlung und Empfehlung von Kontrollmaßnahmen

In dieser Phase sind Überlegungen anzustellen, wie die festgestellten Datenschutzrisiken durch entsprechende Kontrollmaßnahmen minimiert werden können. Diese können technischer oder nicht-technischer Natur sein, wie zB Maßnahmen zur Datenminimierung,

Vorgaben für die Speicherung und Löschung der personenbezogenen Daten, Einsatz von Verschlüsselungsverfahren usw.

Schritt 4: Dokumentation der Schlussfolgerung und der verbleibenden Risiken

Nach Abschluss der Risikoabschätzung ist schlussendlich eine Entscheidung zu treffen, ob die Datenanwendung in der vorliegenden Art betrieben werden darf oder ob noch entsprechende Maßnahmen zur Risikominimierung zu treffen sind.

Der gesamte Prozess der Datenschutz-Folgenabschätzung ist entsprechend zu dokumentieren.

In Bezug auf den Einsatz von Smart Metering hat die EU-Kommission am 10. Oktober 2014 eine Empfehlung „über das Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme“ (2014/724/EU) veröffentlicht. Dieser Empfehlung sind zwei Stellungnahmen der Artikel-29 Datenschutzgruppe, und zwar vom 22. April 2013 (WP 205) und vom 4. Dezember 2013 (WP 209) vorangegangen. Auch dieses Muster kann für die Vornahme einer Datenschutz-Folgenabschätzung herangezogen werden https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

Last but not least ist auch die Herausgabe einer internationalen Norm zu diesem Thema mit der Bezeichnung ISO/IEC 29134 geplant. An dieser Norm wird bereits seit mehreren Jahren gearbeitet, derzeit befindet sie sich im Stadium „30.20 CD study/ballot initiated“, eine Verabschiedung ist mit 30. November 2016 geplant.

ABSCHNITT 4

DATENSCHUTZBEAUFTRAGTER

Artikel 35

Benennung eines Datenschutzbeauftragten

1. *Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann – bzw. sofern im Unionsrecht oder im nationalen Recht vorgesehen, muss – einen Datenschutzbeauftragten benennen (...).*
2. *Eine Gruppe von Unternehmen darf einen gemeinsamen Datenschutzbeauftragten ernennen.*
3. *Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann für mehrere solcher Behörden oder Einrichtungen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.*
4. (...).
5. *Der (...) Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben, namentlich des Nichtvorhandenseins von Interessenkonflikten (...).*
6. (...)
7. (...). *Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 37 nicht mehr erfüllt, außer es liegen schwerwiegende Gründe nach dem Recht des betreffenden Mitgliedstaats vor, die eine Entlassung eines Beschäftigten oder Bediensteten rechtfertigen.*
8. *Der Datenschutzbeauftragte kann Beschäftigter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.*

9. *Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.*

10. *Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.*

11. (...)

Anmerkung: Der Kommissionsentwurf vom 25. Jänner 2012 enthält noch die Bestimmung zur Bestellung eines Datenschutzbeauftragten (DSB) für Unternehmen mit mehr als 250 Mitarbeitern. Diese Bestimmung hat sich – so wie viele andere Bestimmungen der DS-GVO – im Laufe der mehr als dreijährigen Verhandlungsdauer mehrmals geändert. So brachte der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres „LIBE“ unter der Leitung des Berichterstatters Jan Philipp Albrecht in seinem Bericht vom 17. Dezember 2012 ein anderes Entscheidungskriterium für die Ernennung eines DSB ein, nämlich die Verarbeitung von mehr als 500 betroffenen Personen/Jahr. Diesem Kriterium war allerdings kein langes Leben beschieden, da der vom EU-Parlament am 12. März 2014 in Straßburg beschlossene Vorschlag die Anzahl auf mehr als 5.000 betroffene Personen/Jahr erhöhte. Der am 15. Juni 2015 nunmehr veröffentlichte Kompromissvorschlag des Rates zeigt ein mehr als überraschendes Ergebnis. Demnach besteht gem. Abs. 1 nur mehr eine Pflicht zur Ernennung eines DSB, wenn es das EU-Gemeinschaftsrecht oder das Recht des MS erfordert. Ist dies nicht der Fall, dann kann der Auftraggeber oder der Dienstleister diese Funktion auf freiwilliger Basis besetzen. Abs. 1 sieht auch vor, dass ein DSB für mehrere Unternehmen tätig sein kann, zB Konzern-DSB. Diese Bestimmung gilt gem. Abs. 2 auch für

den öffentlichen Bereich. Für den DSB ist gem. Abs. 7 ein spezieller Kündigungsschutz vorzusehen. Aufgrund der Bestimmungen des Abs. 8 ist es auch möglich, einen externen DSB zu ernennen.

Die europaweit verpflichtende Einführung eines DSB war ein Kernpunkt der geplanten europäischen Reform des Datenschutzrechts. Die derzeitige Position der Justiz- und Innenminister sieht aber nunmehr eine Bestellung des DSB auf Basis der Freiwilligkeit vor. Es bleibt abzuwarten, auf welche endgültige Regelung sich EU-Parlament, EU-Kommission und EU-Ministerrat einigen. Bleibt die derzeitige Regelung aufrecht, so ist abzuwarten, wie die österreichische Bundesregierung mit diesem Thema umgeht.

Artikel 36

Stellung des Datenschutzbeauftragten

1. *Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.*

2. *Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 37 und stellt (...) die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung.*

3. *Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben unabhängig handeln kann und keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des für die Ver-*

arbeitung Verantwortlichen oder des Auftragsverarbeiters.

4. Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Anmerkung: Dieser Artikel setzt sich mit den Kompetenzen des DSB auseinander. Demnach sind dem DSB die entsprechenden Ressourcen zur Verfügung zu stellen, damit dieser seine vielfältigen Aufgaben wahrnehmen kann. Bei der Einordnung des DSB in die Unternehmensorganisation ist zu berücksichtigen, dass dieser unabhängig agieren kann und dass er durch seine Tätigkeit keinerlei Nachteile erfährt. Der erste Ansprechpartner des DSB ist der Vorstand oder der Geschäftsführer. Abhängig von der Größe des Unternehmens und der Sensibilität seiner Datenanwendungen ist es möglich, dass der DSB auch andere Tätigkeiten im Unternehmen verrichtet.

Artikel 37

Aufgaben des Datenschutzbeauftragten

1. Dem (...) Datenschutzbeauftragten obliegen (...) folgende Aufgaben:

(a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten (...);

(b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten sowie der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

(c) (...)

(d) (...)

(e) (...)

(f) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 33;

(g) Überwachung von auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutz-beauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;

(h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 34, und gegebenenfalls Beratung zu allen sonstigen Fragen.

2. (...)

2a. Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Anmerkung: Dieser Artikel enthält die vielfältigen Aufgaben des DSB. Neben seiner Tätigkeit als Beratungs- und Schulungsorgan für die Mitarbeiter sowie als „Wächter“ darüber, dass die Datenschutzvorschriften im Unternehmen auch wirklich eingehalten werden, unterstützt er den Auftraggeber bei der Wahrnehmung seiner – der in Kapitel IV Art. 22 DS-GVO – enthaltenen Pflichten, sowie der in Art. 28 geforderten Aufzeichnung über die einzelnen Datenanwendungen und bei der in Art. 33 geforderten Durchführung der Datenschutz-Folgenabschätzungen. Darüber hinaus ist er der primäre Ansprechpartner für die Aufsichtsbehörde.

Artikel 79a
Geldbußen

1. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 250 000 EUR oder im Fall eines Unternehmens 0,5 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen verhängen, der vorsätzlich oder fahrlässig

(a) Anträge der betroffenen Person nicht (...) innerhalb des Zeitraums nach Artikel 12 Absatz 2 beantwortet;

(b) unter Verstoß gegen Artikel 12 Absatz 4 Satz 1 eine Gebühr (...) verlangt.

2. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 500 000 EUR oder im Fall eines Unternehmens 1 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig

(a) der betroffenen Person die Auskünfte gemäß (...) Artikel 12 Absatz 3 sowie den Artikeln 14 und 14a nicht [rechtzeitig oder] in [hinreichend] transparenter Weise erteilt;

(b) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt oder personenbezogene Daten nicht gemäß Artikel 16 berichtet (...);

(c) personenbezogene Daten unter Verstoß gegen das Recht auf Löschung und „Vergessen werden“ nach Artikel 17 Absatz 1 Buchstaben a, b d oder e nicht löscht;

(d) (...)

(da) personenbezogene Daten unter Verletzung des Rechts auf Einschränkung der Verarbeitung nach Artikel 17a verarbeitet oder die betroffene Person nicht vor Aufhebung der Einschränkung nach Artikel 17a Absatz 4 unterrichtet;

(db) unter Verstoß gegen Artikel 17b nicht jeden Empfänger, an den der für die Verarbeitung Verantwortliche personenbezogene Daten weitergegeben hat, über jegliche Berichterung, Löschung oder Einschränkung der Verarbeitung unterrichtet;

(dc) der betroffenen Person unter Verstoß gegen Artikel 18 (...) nicht die sie betreffenden personenbezogenen Daten bereitstellt;

(dd) personenbezogene Daten nach dem Einspruch der betroffenen Person gemäß Artikel 19 Absatz 1 verarbeitet, es sei denn, er kann (...) zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, (...) Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;

(de) der betroffenen Person nicht gemäß Artikel 19 Absatz 2 Informationen über das Recht übermittelt, gegen eine Verarbeitung für Zwecke der Direktwerbung Einspruch einzulegen, oder unter Verstoß gegen Artikel 19 Absatz 2a die Verarbeitung von Daten auch nach einem Einspruch der betroffenen Person fortsetzt;

(e) die jeweilige Verantwortung der gemeinsam für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt;

(f) die Dokumentation gemäß Artikel 28 und Artikel 31 Absatz 4 nicht oder nicht hinreichend gewährleistet.

(g) (...)

3. Die Aufsichtsbehörde (...) kann eine Geldbuße, die 1 000 000 EUR oder im Fall eines Unternehmens 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres nicht überschreitet, gegen einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter verhängen, der vorsätzlich oder fahrlässig

(a) personenbezogene Daten ohne (...) Rechtsgrundlage verarbeitet oder die Bedingungen für die Einwilligung gemäß den Artikeln 6, 7, 8 und 9 nicht beachtet;

(b) (...);

(c) (...);

(d) die Bedingungen gemäß Artikel 20 in Bezug auf (...) eine automatisierte Entscheidung;

(e) die Bedingungen gemäß Artikel 20 in Bezug auf (...) eine automatisierte Entscheidung;

dungsfindung einschließlich Profiling nicht beachtet;

(da) (...) keine geeigneten Maßnahmen trifft oder nicht in der Lage ist, die Einhaltung der Anforderungen (...) nachzuweisen, wie dies in den Artikeln 22 (...) und 30 vorgesehen ist;

(db) unter Verstoß gegen Artikel 25 keinen Vertreter benennt;

(dc) unter Verstoß gegen Artikel 26 (...) personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;

(dd) die Aufsichtsbehörde bei einer Verletzung des Schutzes personenbezogener Daten nicht alarmiert oder sie oder die betroffene Person unter Verstoß gegen die Artikel 31 und 32 nicht [rechtzeitig oder nicht] vollständig von einer solchen Verletzung benachrichtigt;

(de) unter Verstoß gegen Artikel 33 keine Datenschutz-Folgenabschätzung vornimmt oder personenbezogene Daten unter Verstoß gegen Artikel 34 ohne vorherige Zurateziehung der Aufsichtsbehörde verarbeitet;

(e) (...);

(f) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht oder die in den Artikeln 38a und 39a festgelegten Bedingungen und Verfahren nicht einhält;

(g) unter Verstoß gegen die Artikel 41 bis 44 eine Datenübermittlung an einen Empfänger in einem Drittland oder an eine internationale Organisation vornimmt oder anordnet;

(h) einer Anweisung oder einer vorübergehenden oder endgültigen Einschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1b nicht Folge leistet oder unter Verstoß gegen Artikel 53 Absatz 1 keinen Zugang gewährt.

(i) (...)

(j) (...).

3a. Verstößt ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen mehrere der in den Absätzen 1, 2 oder 3 aufgeführten Bestimmungen dieser Verordnung, so darf der Gesamtbetrag der Geldbuße den Betrag für den schwerwiegendsten Verstoß nicht übersteigen.

4. (...)

Anmerkung: Während Art. 79 allgemeine Bedingungen für die Verhängung von Geldbußen enthält, werden diese in Art. 79a konkretisiert. Der Art. 79a enthält einen umfassenden Katalog von Tatbeständen. Die Höhe der Geldbußen wurde zwar im Vergleich zu den am 12. März 2014 vom Plenum des EP angenommenen Kompromiss-Paketes, welches noch als Höchststrafe EUR 100 Mio. oder 5 % des weltweiten Umsatzes vorsah, erheblich reduziert, kann aber mit einer nunmehr vorgesehenen Geldbuße von höchstens EUR 1 Mio. oder 2 % des weltweiten Umsatzes nach wie vor für Unternehmen existenzbedrohlich sein.

••••

Unser nächstes Seminar

„Datenschutz im modernen Unternehmen – Vom Gesetzestext bis zur unternehmenskonformen Umsetzung“

findet am 3. November 2015 statt.

Es referiert der Mitautor des Standardwerkes zum österreichischen DSG:

Prof. KommR Hans-Jürgen Pollirer.

Anmeldung unter www.secur-data.at oder telefonisch unter (01) 533 42 07-0.