PGDS - 15100 - 2/62
bis 21.6.

Loose, Katrin

Von: Huppertz, Marie-Therese [marie-therese.huppertz@sap.com]
Gesendet: Freitag, 11. Mai 2012 14:11
An: StRogall-Grothe_
Cc: Stentzel, Rainer, Dr.
Betreff: Stellungnahme zur EU Datenschutzverordnung
Anlagen: EU DatenschutzVO-SAP Stellungnahme.pdf

Sehr geehrte Frau Staatssekretärin Rogall Grothe,

das Thema Datenschutz ist für die SAP von größter Bedeutung. Wir begrüßen nachdrücklich, dass die EU Kommission eine Harmonisierung des Datenschutzrechtes in Europa anstrebt und unterstützen ihren Ansatz, dies über eine Datenschutzgrundverordnung zu tun. Jedoch enthält der Verordnungsentwurf eine Vielzahl von Bestimmungen, die einen erheblichen Mehraufwand für die für den Datenschutz verantwortlichen Stellen bedeuten würde ohne gleichzeitig das Datenschutzniveau zu verbessern.

In unserer beiliegenden Stellungnahme gehen wir ausführlich auf die Punkte ein, bei denen aus unserer Sicht Nachbesserungsbedarf besteht. Wir hoffen, dass unsere Anregungen dazu beitragen im Dialog eine Regelung zu finden, die ein hohes Datenschutzniveau für die Bürger Europas sicherstellt und gleichzeitig die Innovations- und Wettbewerbsfähigkeit der Europäischen IKT Unternehmen unterstützt.

Gerne stehe ich Ihnen für weiterführende Gespräche jederzeit zur Verfügung.

Mit freundlichen Grüßen,

Marie-Therese Huppertz

Fr. Heltrom z.K. 14/5 1) Frau StnRG a.d. Einpang vorgelegt 8/29/5 → PGDS fr 17/5 2) Herrn AL V z.w.V. 3) Ø Herrn IT-D → Bertram 11/5 14/5.

Marie-Therese Huppertz
Vice President I Government Relations I Global Communications
SAP AG I Rosenthaler Strasse 30 I 10178 Berlin I Germany
T +49 30 41092 - 240 I F +49 6227 78-48711 I M +49 151 57 118221I mailto:marie-therese.huppertz@sap.com
www.sap.com

Stellungnahme

zum Vorschlag der EU Kommission für eine Datenschutzgrundverordnung vom 25.1.2012

(KOM 2012) 9 Final

Die SAP AG begrüßt nachdrücklich die Initiative der EU Kommission zur Harmonisierung des Datenschutzrechtes in Europa. Als weltweit in über 160 Ländern tätiger Produzent von Business-Software unterstützen wir die Schaffung eines einheitlichen Rechtsrahmens in Europa. Eine Harmonisierung der fragmentierten Datenschutzbestimmungen würde das Angebot und auch die Nutzung von IKT- Dienstleistungen in der EU deutlich erleichtern. Ein einheitlicher Rechtsrahmen liefert somit auch einen wichtigen Baustein zur Verbesserung der Wettbewerbsfähigkeit der europäischen IKT – Industrie insbesondere im weltweit wachsenden Cloud-Computing Markt. In der Studie[1] „Survival of the Fittest", die 2011 gemeinsam von Roland Berger und der SAP AG vorgelegt wurde, gehen wir insbesondere auf die Herausforderungen des Datenschutzes im Cloud-Computing Markt ein. Auf die in der Studie entwickelten Vorschläge zur Harmonisierung und zur Zertifizierung von Cloud Lösungen möchte ich in diesem Zusammenhang nochmals ausdrücklich hinweisen.

Moderne Systeme der Datenverarbeitung sind heute aus den Abläufen eines effizient gesteuerten Unternehmens wie auch aus der öffentlichen Verwaltung oder anderen Organisationen nicht mehr weg zu denken. Sie erfordern Technologie-offene Regelungen, die technische Innovationen fördern und den internationalen Charakter der sich ausweitenden weltweit vernetzten Wirtschaftsabläufe berücksichtigen.

Die tägliche Verarbeitung von personenbezogenen Daten für unsere Kunden macht die SAP AG zu einem der größten datenverarbeitenden Unternehmen weltweit. Der sichere und hochvertrauliche Umgang mit diesen Daten unter Beachtung von geltenden nationalen und europäischen datenschutzrechtlichen Vorschriften bildet die Basis für unseren Erfolg.

Uns liegen die Wahrung eines hohen Niveaus des Schutzes personenbezogener Daten sowie ein hohes Maß an Sicherheit bei der Verarbeitung dieser Daten am Herzen. Dies muss jedoch einhergehen mit der Bewahrung der Innovationsfähigkeit unserer Wirtschaft, denn nur sie kann die langfristige internationale Wettbewerbsfähigkeit insbesondere im Bereich der IKT – Industrie sichern. Diese Branche ist jedoch wie keine andere einem extremen internationalen Wettbewerbsdruck ausgesetzt.

Viele Entwicklungen, die sich in der vorliegenden Verordnung niederschlagen, sind SAP als globalem Unternehmen mit Hauptsitz in Deutschland nicht fremd. Gerade im Zuge zunehmender Waren-, Personen- und eben auch Daten-Mobilität müssen bestehende rechtliche Hürden überwunden werden. Daher ist die avisierte Harmonisierung ein wichtiger Schritt in die richtige Richtung.

Der Verordnungsentwurf enthält allerdings leider auch eine Vielzahl von Bestimmungen, die einen erheblichen Mehraufwand für die verantwortlichen Stellen und die Auftragsdatenverarbeiter bedeuten würden, ohne gleichzeitig das Datenschutzniveau zu verbessern. Hier besteht aus Sicht der SAP dringender Nachbesserungsbedarf.

Deshalb erlauben wir uns, folgende Anregungen zur Verbesserung des vorliegenden Vorschlages in die Diskussion einzubringen. Gleichzeitig möchten wir betonen, dass SAP die konkreten Änderungsanträge in den Positionspapieren von Digital Europe und BITKOM unterstützt:

1. Vollharmonisierung – ja, Überregulierung – nein

Unternehmen benötigen transparente und einheitliche Datenschutzregelungen, die Rechtssicherheit garantieren und administrative Hürden minimieren. Die SAP AG begrüßt daher die Wahl einer Verordnung anstelle einer Richtlinie zur vollständigen Harmonisierung des Datenschutzrechts in Europa. Die SAP befürwortet zudem, dass notwendige Konkretisierungen der zukünftigen Verordnung durch „delegierte Rechtsakte" der Europäischen Kommission vorgenommen werden sollen, damit die Harmonisierung gewährleistet bleibt. Allerdings ist aus unserer Sicht fraglich, ob eine Konkretisierung tatsächlich in all den Bereichen notwendig ist, wie sie im Verordnungsentwurf der Kommission vorgesehen ist. Eine derartige Flut von delegierten Rechtsakten könnte zum einen zu einer Überregulierung führen, welche Innovation und Wettbewerbsfähigkeit im digitalen Europa hemmen. Zum anderen könnte die Vielzahl von delegierten Rechtsakten die Rechtssicherheit einschränken. Insbesondere der sich entwickelnde Markt für Cloud- Dienstleistungen erfordert klare, verbindliche und standardisierte Regelungen für alle Bereiche der Privatwirtschaft und wesentliche Teile relevanter öffentlicher Stellen. Nur so kann man den europäischen Cloud-Anbietern eine Chance zur Entwicklung dieses Marktes eröffnen. Hier erscheinen insbesondere die zahlreich vorgesehenen Durchführungsverordnungen aufgrund der bereits detaillierten Kriterien in den Art. 22, 26 und 28 unangebracht. Hiervon sollte Abstand genommen werden, um möglichst früh Rechtssicherheit zu gewährleisten. In der Vergangenheit hat sich gezeigt, dass sich vorbildliche Verfahren (Best Practices) und internationale Standards etablieren, die sowohl die notwendige Flexibilität als auch eine breite Anerkennung bei Unternehmen und Behörden finden.

Des Weiteren sind die Ansätze zur Konzernregulierung (z.B. gemeinsam für die Verarbeitung Verantwortliche) nicht ausreichend. Die Verordnung sollte existierende Verbindungen und Abhängigkeiten in internationalen Konzernen berücksichtigen. Die Organisation von Unternehmen in Konzernstrukturen ist eine Realität, die vom Datenschutzrecht nicht ignoriert werden darf. Es ist zu wenig, nur für den Transfer von personenbezogenen Daten in Drittstaaten innerhalb von Konzernen ein Instrument wie die verbindlichen unternehmensinternen Vorschriften vorzusehen. Vielmehr sollte das Konzept der „gemeinsam für die Verarbeitung Verantwortliche", das sowohl in der Definition des für die Verarbeitung Verantwortlichen (Art. 4 Abs. 5) als auch im Artikel 24 angelegt ist, auf Unternehmensgruppen nach Art.4 Abs. 16 und 17 ausgeweitet werden. Dazu könnte Artikel 24 wie folgt ergänzt werden:

> „(2) Sofern Konzerne als gemeinsamer für die Verarbeitung Verantwortlicher Auftraggeber auftreten, sollten die nach Art.22 Abs.1 vorgesehenen Maßnahmen und Strategien gleichermaßen im für die Verarbeitung Verantwortlichen Unternehmen wie auch im kontrollierten Unternehmen".
>
> „(2) If Groups of Undertakings act as Joint Controllers, policies and measures according to Paragraph 1 of Art. 22 shall be implemented in the controlling and the controlled undertakings equally."

Es ist zudem nicht klar, ob auch Konzerne vom One-Stop-Shop nach Art. 51. Abs. 2 bezüglich der Datenschutzaufsicht profitieren können. Wenn sich die One-Stop-Shop Regelung nur auf die Zuständigkeit bei unselbständigen Niederlassungen bezieht, bietet sie keinerlei Erleichterung für große Unternehmen, die regelmäßig Konzernstrukturen besitzen.
Darüber hinaus enthält der Verordnungsentwurf selbst viele Bestimmungen, deren Relevanz für den Datenschutz fraglich ist, die aber einen erheblichen Mehraufwand für den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter bedeuten. Hier sind in erster Linie die überbordenden Dokumentationsvorschriften z. B. im Artikel 28 zu nennen, die weit über die bestehenden Vorschriften, beispielsweise im Bundesdatenschutzgesetz, hinausgehen.

Die Anlage enthält eine Übersicht dieser aus Sicht der SAP überbordenden bürokratischen und teilweise praxisfernen Bestimmungen des vorliegenden Verordnungsentwurfs.

2. **Das deutsche Modell des betrieblichen Datenschutzbeauftragten hat sich in der Praxis bewährt.**

Die SAP AG begrüßt ausdrücklich die Einführung des betrieblichen Datenschutzbeauftragten in Europa. Das seit Jahren in Deutschland praktizierte Selbstregulierungsmodell hat sich bewährt und sollte auf die europäische Ebene übertragen werden. Die Bestimmungen in dem Verordnungsentwurf der Europäischen Kommission führen jedoch leider zu einer Aushöhlung der Befugnisse des betrieblichen Datenschutzbeauftragten und zerstören damit ein gut funktionierendes Verfahren der unbürokratischen und effizienten Regelung von datenschutzrechtlichen Fragestellungen im Unternehmen.

Hier einige konkrete Beispiele:

Ein großer Vorteil des nationalen Datenschutzbeauftragten in Deutschland ist die Wahrnehmung der Vorabkontrolle. Art. 34 Abs. 2, 4 und 6 ersetzen diese Vorabkontrolle des Datenschutzbeauftragten jedoch durch eine vorherige Genehmigung der Aufsichtsbehörden, die einen deutlich höheren Aufwand erfordert. Damit setzt die Verordnung auf überbordende bürokratische Vorschriften, um die generell begrüßenswerten Ziele zu erreichen.

Des Weiteren stellt die Genehmigung auch des Auftragsverarbeiters, wie in Art. 34 vorgesehen, eine unangemessene Doppelung dar und sollte gestrichen werden.

Art. 37 der Verordnung geht sogar so weit, die Arbeitsaufläufe des betrieblichen Datenschutzbeauftragten im Detail mit weiteren Dokumentations- und Informationsverpflichtungen (Art. 14) auszugestalten. Dies ist unsachgemäß und läuft dem Gedanken der Selbstregulierung zuwider.

3. **Zertifizierungsmechanismen unterstützen**

Art. 39 des vorliegenden Verordnungsvorschlages bietet einen ausgezeichneten Rahmen dafür, die Selbstregulierung und Zertifizierung noch weiter voranzutreiben und hierfür einen praxisgerechten Rechtsrahmen vorzuzeichnen. Wie bereits in der Studie „Survival of the Fittest"[ii] dargelegt, sehen wir in der Etablierung eines europaweiten Datenschutz-Zertifikats ein wichtiges Instrument, um Vertrauen in die Sicherheit und den Schutz der Daten bei den angebotenen Cloud-Dienstleistungen zu fördern.

Analog zu den in Art. 38 für die Verhaltensregeln geltenden Regelungen sollten Verbände und Unternehmen zusätzlich die Möglichkeit erhalten, der Europäischen Kommission diese Zertifikate vorzulegen. Die Kommission sollte dann befugt sein, Durchführungsbestimmungen zu erlassen, die eine europaweite Gültigkeit der präsentierten Zertifikate in der gesamten Europäischen Union vorsehen. Analog zur Regelung für Verhaltensregeln sollte die Verordnung eine derartige verbindliche Anerkennung von Zertifikaten vorsehen. Damit könnte ein Anreiz zur Entwicklung dieser Mechanismen entwickelt werden, der zu mehr Rechtssicherheit und mehr Transparenz im Cloud Computing Markt führen wird.

Gleichzeitig könnte die Europäische Kommission die Aushandlung von internationalen Normen und Selbstkontrollmechanismen, wie z.B. eines ISO Standards, vorantreiben.

4. **Angemessener Sanktionskatalog**

Die Einführung strenger Sanktionen kann grundsätzlich der Durchsetzung eines höheren Datenschutzniveaus dienen. Die vorliegenden Vorschläge schießen jedoch weit über dieses Ziel hinaus. Die vorgesehenen Sanktionen, deren Anknüpfungspunkte häufig auf unbestimmte Rechtsbegriffe verweisen, führen für Unternehmen zu einer unverhältnismäßigen und möglicherweise existenzbedrohenden Situation. (Beispiele aus Art. 79 für unbestimmte Rechtsbegriffe: „ ... Auskünfte ... in nicht *hinreichend* transparenter Weise erteilt ... die jeweilige Verantwortung der für die Verarbeitung Mitverantwortlichen

nicht oder nicht *hinreichend* gemäß Artikel 24 bestimmt hat ... ohne *ausreichende* Rechtsgrundlage ... keine *geeigneten* Maßnahmen gemäß den Artikeln 22, 23 und 30 anwendet ...)

Diese problematischen Ansätze sollten sowohl von den eine Sanktion begründenden Tatbeständen wie auch der Kalkulationsmethode der Höhe der Sanktion überdacht werden.

5. Auftragsdatenverarbeitung

Die SAP AG betreibt, wie bereits eingangs dargestellt, in großem Umfang Datenverarbeitungen für viele Auftraggeber aus privaten Unternehmen und öffentlichen Einrichtungen. Für diese Verfahren sind klare Regeln in Bezug auf die Rechte und Pflichten von Auftraggeber und Verarbeiter von großer Bedeutung.

Positiv hervorzuheben ist die avisierte Harmonisierung der Zuständigkeiten in nur einer nationalen Aufsichtsbehörde je für die Verarbeitung Verantwortlichem bzw. Auftragsverarbeiter.

Leider wird jedoch die Beziehung zwischen dem für die Verarbeitung Verantwortlichem und dem Auftragsverarbeiter nicht ausreichend klar geregelt. Dies erscheint jedoch gerade im Hinblick auf den Ausbau der Cloud- Dienstleistungsangebote von großer Bedeutung.

Hier einige Beispiele:

Die Artikel 22,24,26, 27, 28 des Verordnungsentwurfs lassen Klarheit darüber vermissen, wie die Verantwortlichkeiten zwischen den Parteien verteilt sind. Fraglich ist zum Beispiel, welche rechtlichen Konsequenzen die Unterstützungspflicht haben soll, die bisher als Teil der vertraglichen Regelungen den Vertragsparteien überlassen wurde. (Art. 26 Abs. 2 (f)).

SAP setzt hier auf bewährte vertragliche Regelungen zwischen den jeweiligen Vertragspartnern.

Die SAP fordert eine klare Regelung in der Verordnung, wonach wie bisher ausschließlich der für die Verarbeitung Verantwortliche für die rechtmäßige Verarbeitung von personenbezogenen Daten verantwortlich bleiben soll. Die Aufgaben und Verantwortlichkeiten des Auftragsverarbeiters sollten dagegen weitgehend vertragsrechtlich zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter geregelt werden.

Wie bereits unter Punkt 1 dargelegt, erscheinen die zahlreich vorgesehenen Durchführungsverordnungen aufgrund der bereits detaillierten Kriterien in Art. 22, 26 und 28 unangebracht. Der wachsende Cloud-Computing Markt erfordert Rechtssicherheit und Transparenz, die nur dadurch gewährleistet werden kann, dass die Akteure die geltenden Regelungen kennen und sich nicht ständig ändernden Ausführungsbestimmungen ausgesetzt sehen. Eine derartige Unsicherheit würde die notwendigen Investitionen hemmen und die Entwicklung der Cloud-Angebote in Europa verhindern.

ANLAGE

Neue bürokratische Hürden

1. Personenbezug

Die Definition des Personenbezugs in Art. 4 des Verordnungsvorschlages ist derzeit nicht präzise gefasst und führt dazu, dass jedes Datum, nicht nur personenbezogene Daten in den Anwendungsbereich der Verordnung fallen. Dies beruht auf der geänderten Definition der „betroffenen Person". Hier zählt nicht die Identifizierbarkeit durch den für die Verarbeitung Verantwortlichen, sondern durch „jede sonstige natürliche oder juristische Person" (Art. 4 Abs. 1). Da nicht festgestellt werden kann, ob Dritte eine bestimmte Person anhand derer Daten unter unbekannten Umständen identifizieren können, gibt es keine trennscharfe Definition personenbezogener Daten. Entsprechend müssten alle Daten als personenbezogen behandelt werden, für die kein eindeutiger Ausschluss des Personenbezugs möglich ist.
Es scheint jedoch sinnvoll, den Begriff auf tatsächlich relevante Verarbeitungsvorgänge personenbezogener Daten zu beschränken. Gleichzeitig könnten Anreizsysteme für Pseudonymisierung und Anonymisierung geschaffen werden.

2. *Einwilligung*

Die in diversen Artikeln des Verordnungsentwurfs (Art. 4, 6, 7, 17) vorgeschlagenen Regelungen betreffend die Einwilligung müssen entweder als zu pauschal oder als zu restriktiv angesehen werden und damit zu weiteren Unsicherheiten führen.

3. Recht auf Vergessenwerden

Das Recht ist mit den bisherigen Geboten zur Löschung von Daten nach Erfüllung der ursprünglichen Zwecke bereits ausreichend erfüllt und sollte gestrichen werden. Die Festlegungen zum Löschen sind auch ohne dieses Schlagwort ausreichend definiert.

4. Informationspflichten

Die in Art. 11 enthaltenen Informationspflichten sind zu unbestimmt und führen zu Rechtsunsicherheit.

5. Prozesse und Verfahren zur Wahrnehmung der Rechte des Datensubjektes

- Art. 12 verlangt umfangreiche Prozessdefinitionen, unabhängig von der Wahrscheinlichkeit der Anforderungen. Wir plädieren dafür, es den Unternehmen zu überlassen, wie sie die zur Ausübung der Rechte der Betroffenen erforderlichen Prozesse organisieren.
    - Art. 12 Abs. 2 (*Antrag in elektronischer Form*) verkennt die Schwierigkeit, einen Betroffenen online zu identifizieren.
    - Art. 12 Abs. 6 erlaubt der Europäischen Kommission, den Unternehmen detaillierte Vorgaben zu Formblättern und internen Verfahren zu machen, und greift damit unangemessen in die Organisationsfreiheit der Unternehmen ein.
- Art. 13 schafft weitere Pflichten zur Datenspeicherung, denn er impliziert eine umfangreiche Dokumentation jeder Datenübermittlung, die im Zusammenhang mit den Art. 16/17 spezifiziert werden muss, was zu übermäßiger Bürokratie und Kosten führen wird.
- Art. 14 verlangt nicht nur die Identifikation des für die Verarbeitung Verantwortlichen, wie schon bisher, sondern die Nennung des Datenschutzbeauftragten und ggf. des Vertreters des Unternehmens. Das bringt im Einzelfall wenig, da sich Namen ändern können und eine Aktualisierung unzumutbar wäre. Eine Post- und E-Mail-Adresse für die Funktion „Datenschutzbeauftragter" muss ausreichen. Eine Veröffentlichung auf der Homepage wäre ebenfalls akzeptabel, da eine zentrale Aktualisierung möglich wird.

- Art. 15 (*Auskunftsrecht*) Abs. 4 räumt der Europäischen Kommission das Recht ein, bürokratische Vorgaben zu Formblättern und Prozessen der Unternehmen zu machen. Auch hier wird die Organisationsfreiheit der Unternehmen unangemessen eingeschränkt.

6. Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
Wie bereits eingangs erwähnt, sind die in diesem Abschnitt des vorliegenden Verordnungsentwurfs vorgeschlagenen Regelungen betreffen die Rechte und Pflichten zwischen beiden Parteien nicht klar gefasst und könnten zu einer Flut von Rechtsstreitigkeiten führen. Außerdem werden unverhältnismäßig weitreichende neue bürokratische Prozesse vorgeschrieben, die zu einem kostspieligen Mehraufwand führen werden, ohne dabei das Schutzniveau zu erhöhen.

Im Einzelnen:

Art. 22 (*Pflichten des für die Verarbeitung Verantwortlichen*) definiert eine Vielzahl bürokratischer Anforderungen, die in der Vergangenheit von den Unternehmen als „Best Practice" verstanden wurden, um sich von den gesetzlichen Anforderungen positiv abzusetzen. Jetzt wird die „Übererfüllung" zur Regel.
Beispiele:
- Dokumentation nach Art. 28
- Datenschutz- Folgenabschätzung nach Art. 33
- Vorherige Genehmigung und vorherige Zurateziehung nach Art. 34
- Implementierung einer Art Datenschutzmanagementsystems nach Art. 22 (3)
- Unsicherheit durch delegierte Rechtsakte „um etwaige weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für die in Absatz 1 genannten Maßnahmen ... festzulegen"

Art. 28 Dokumentation geht weit über die Anforderungen des BDSG zum Verfahrensverzeichnis hinaus.

<u>Melde- und Benachrichtigungspflichten</u>

Art. 31 geht weit über das Erforderliche hinaus. Eine generelle Meldepflicht für jedweden Datenverlust, unabhängig davon, ob es sich um sensible Daten handelt oder ob schwerwiegende Beeinträchtigungen drohen, ist nicht sachgerecht. Der aktuelle Vorschlag führt dazu, dass Unternehmen z.B. jeden Verlust eines Mobiltelefons der Aufsichtsbehörde melden müssten. Die Kohärenz mit der geltenden ePrivacy Richtlinie (Art. 4 Abs. 3 http://ec.europa.eu/justice/data-protection/law/ files/recast_20091219_en.pdf) erfordert den Verzicht auf die 24-Stunden-Frist zur Meldung einer Datenlücke. Neben dem unkalkulierbaren Aufwand auf Seiten der Aufsichtsbehörden stellen diese Regelungen auch einen Eingriff in die Selbstregulierungsmechanismen der Unternehmen oder anderer Stellen dar und würden auch für diese Unternehmen sowohl auf Seiten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters einen bürokratischen Mehraufwand verursachen, der weder mehr Sicherheit noch einen besseren Schutz der Daten nach sich ziehen würde. Vielmehr sollte dem für die Verarbeitung Verantwortlichen die Wahl der zur Schließung der Datenlücke gebotenen Maßnahmen vorbehalten bleiben.

Die 24 Stunden Meldepflicht sollte deshalb durch „unverzüglich" ersetzt werden.

Fraglich ist zudem, ob die Aufsichtsbehörden auch zu einem Dienst an Wochenenden und Feiertagen verpflichtet sind, um eine Meldung jederzeit entgegennehmen zu können.

Es gibt keinerlei Beurteilungsspielraum, den der § 42a BDSG sinnvollerweise bietet. Selbst wenn nach menschlichem Ermessen keine Gefahr einer unrechtmäßigen Kenntnisnahme besteht, muss gemeldet werden. Auch die Entscheidung, Betroffene nicht zu informieren, obliegt allein der Aufsichtsbehörde (Art. 32 Abs. 3).

Ferner sollte die Europäische Kommission im Hinblick auf die gebotene Rechtssicherheit von der Möglichkeit zukünftiger Durchführungsverordnungen Abstand nehmen.

Datenschutz-Folgenabschätzung

Art. 33 *Datenschutz-Folgenabschätzung*: Die Vorschriften entsprechen teilweise dem § 4d Abs. 5 BDSG, sind aber deutlich bürokratischer angelegt. Der zu erwartende delegierte Rechtsakt wird sicherlich auch nicht zur Vereinfachung beitragen.

Während das BDSG eine klare Regelung enthielt, nach der nur der für die Verarbeitung Verantwortliche zur Vorabkontrolle verpflichtet war, wird nun die Datenschutz-Folgenabschätzung dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter auferlegt. Wie dies im Falle von Cloud Services geregelt wird, ist unsicher. Hier könnte eine Verschiebung der Verantwortlichkeit auf den Auftragsverarbeiter erfolgen. Hier haben sich die im Rahmen der Auftragsdatenverarbeitung entwickelten Regelungen bewährt und sollten erhalten bleiben. Natürlich wird jeder Datenverarbeiter zu einer Unterstützung des Auftraggebers bereit sein, wenn die Verantwortlichkeiten klar definiert bleiben.

Abs. 4 schreibt vor, die Meinung der Betroffenen oder ihrer Vertreter einzuholen. Dies ist ein Punkt, der durchaus sinnvoll sein kann, aber der Entscheidung der verantwortlichen Stelle überlassen bleiben soll, die immer schutzwürdige Belange der Betroffenen abwägen muss. Es besteht kein Grund, diese Abwägung ohne Not bürokratisch zu regeln.

Art. 34 *vorherige Genehmigung und vorherige Zurateziehung*: Einer der großen Vorteile des BDSG ist die Übertragung der Kompetenz der Vorabkontrolle an den Datenschutzbeauftragten. Art. 34 Abs. 2, 4 und 6 ersetzen die Vorabkontrolle des Datenschutzbeauftragten durch Entscheidungen der Aufsichtsbehörden, die auch formal einen deutlich höheren Aufwand erfordern. Die Kompetenz des Datenschutzbeauftragten im Umfang des BDSG sollte voll und ganz erhalten bleiben.

7. Datenschutzbeauftragter

Art. 35: Die *Benennung eines Datenschutzbeauftragten* ist grundsätzlich zu begrüßen, aber die Bestelldauer von 2 Jahren ist zu kurz, um der Institution des DSB die erforderliche Verlässlichkeit auch im Verhältnis zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter zu geben. Auch hier ist die Lösung des BDSG praxisgerechter, sie hat sich seit 1977 bewährt.

Art. 37 *Aufgaben des Datenschutzbeauftragten*: Nach bewährtem Muster des BDSG erhält der Datenschutzbeauftragte die Aufgaben der Information und der Kontrolle der verantwortlichen Stellen. Abs.1 (d) ist hier vollständig fremd, da bezogen auf die Dokumentation ein „Sicherstellen" verlangt wird. Auch hier sollte die Verantwortung bei der verantwortlichen Stelle bleiben.

8. Konzernregelung

Art. 51 *Zuständigkeit*: Die One Stop Regelung sollte auch auf Konzerne anwendbar sein und nicht nur auf Unternehmen mit unselbständigen Niederlassungen. Dies würde, wie bereits ausgeführt, zu einer echten Erleichterung führen.

9. Sanktionen

Art. 73 *Recht auf Beschwerde bei einer Aufsichtsbehörde*: Das Verbandsklagerecht wird vermutlich zu einem starken Anstieg von Beschwerden und öffentlicher Aufmerksamkeit führen, insgesamt wird damit die Ausübung von Grundrechten zu einem politischen Spielfeld der Verbände. (s.a. Art. 76 *Gemeinsame Vorschriften für Gerichtsverfahren*)

Art. 79 *Verwaltungsrechtliche Sanktionen*: Der Bußgeldrahmen wurde signifikant erhöht, was sicher grundsätzlich dazu beitragen kann, ein höheres Schutzniveau zu erzielen. Problematisch ist jedoch, dass die eine Sanktion begründenden Tatbestände nicht klar gefasst sind und somit zu Rechtsunsicherheit führen. Außerdem stellt der Bußgeldrahmen nicht nur auf die eigentlichen Verstöße gegen die Rechte der Betroffenen ab, sondern es soll auch jegliche Form von unrechtmäßiger Verarbeitung oder expliziter Missbrauch personenbezogener Daten sanktioniert werden und darüber hinaus jeder Verstoß gegen die überschießenden bürokratischen Regularien:

Art. 79 Abs. 5 (€ 500.000,- oder 1 % des Umsatzes)

- keine Vorkehrungen trifft, um die Einhaltung der Fristen zu gewährleisten;
- die jeweilige Verantwortung der für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt hat;
- die Dokumentation gemäß Artikel 28, Artikel 31 Absatz 4 und Artikel 44 Absatz 3 nicht oder nicht hinreichend gewährleistet

Art. 79 Abs. 5 (€ 1.000.000,- oder 2 % des Umsatzes)

- keine internen Datenschutzstrategien festlegt oder keine geeigneten Maßnahmen gemäß den Artikeln 22, 23 und 30 anwendet, um die Beachtung der Datenschutzvorschriften sicherzustellen und nachzuweisen;
- keine Datenschutz-Folgenabschätzung nach Artikel 33 vornimmt

---

[i] http://www.rolandberger.com/media/publications/2011-11-22-rbsc-pub-Survival_of_the_fittest.html
[ii] Siehe Fußnote i)