Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Dezember 2011 Ausgabe Nr. 66/67

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

Wie wir Sie bereits in unserer Ausgabe Nr. 64 / 65 informiert haben, hat die Europäische Kommission am 4. November 2010 eine Mitteilung für ein Gesamtkonzept für den Datenschutz in der EU [KOM (2010) 609 endg] veröffentlicht.

Grund für diese Aktion sind die neuen vielfältigen Herausforderungen für den Datenschutz, in erster Linie bedingt durch die Dynamik iZm Internetanwendungen mitsamt den modernen Technologien wie soziale Netzwerke oder Cloud Computing.

Dieses Gesamtkonzept gibt Lösungsansätze und Ziele vor und dient als Grundlage für die Ausarbeitung eines Vorschlages, mit dem Ziel, die bestehenden Datenschutzvorschriften entsprechend zu ändern und auf die heutigen datenschutzrechtlichen Anforderungen anzupassen. Auf Basis dieses Konzeptes hat die Europäische Kommission nunmehr einen Vorschlag mit Rechtsvorschriften erarbeitet.

*Die zuständige EU-Justizkommissarin und Vizepräsidentin der EU-Kommission, Viviane Reding, plante den Entwurf der neuen EU-Datenschutzverordnung erst am **25. Jänner 2012** zu präsentieren, jedoch wurde auf www.statewatch.org ein geleakter Entwurf bereits am Mittwoch den 7. Dezember 2011 mit der Bezeichnung „Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Text with EEA relevance) Version 56 (29/11/2011)“ bekannt.*

Dieser Entwurf, der derzeit nur in englischer Sprache vorliegt, umfasst 116 Seiten und kann bei Interesse unter anderem unter der Adresse www.statewatch.org heruntergeladen werden.

Im Folgenden wollen wir auf die aus unserer Sicht wichtigsten Änderungen im Vergleich zur Richtlinie 95/46/EG eingehen, wobei die wohl wichtigste Änderung in der Tatsache liegt, dass an Stelle einer Richtlinie nunmehr eine Datenschutzverordnung treten soll.

***Richtlinien** sind gemäß Art 189 Abs. 3 EWGV bzw. Art 161 Abs. 3 EAGV für den Mitgliedstaat an den sie gerichtet sind **nur** hinsichtlich des zu erreichenden Zieles verbindlich, während die Wahl der Form und der Mittel den innerstaatlichen Stellen überlassen bleibt.*

***Verordnungen** iSd Artikel 189 Abs. 2 EWGV und Art 161 Abs. 2 EAGV besitzen dagegen allgemeine Geltung und sind in allen Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.*
Nun zum Dokument selbst:

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

Version 56
(29/11/2011)

Erläuterungen

1. Hintergrundinformationen zum Vorschlag

Hier weist die Kommission zunächst auf die derzeitigen Grundlagen des europäischen Datenschutzes hin, nämlich auf die RL 95/46/EG und den Rahmenbeschluss 2008/977/JHA. Sie verweist weiters auf Art. 16 des Vertrages über die Arbeitsweise der EU (AEUV) idF aufgrund des am 1. Dezember 2009 in Kraft getretenen Vertrages von Lissabon, als Rechtsgrundlage hin und nimmt auch Bezug auf Art. 8 der EMRK. Schlussendlich weist sie auf die hinlänglich bekannten Schwächen des derzeitigen europäischen Datenschutzrechtes hin, hier im Besonderen auf die mangelhafte Harmonisierung, die bestehenden Rechtsunsicherheiten, sowie die weit verbreitete öffentliche Wahrnehmung über das Bestehen erheblicher Risiken bei Online-Aktivitäten.

2. Ergebnisse der Beratungen mit interessierten Parteien und Folgeabschätzungen

Dieses Kapitel setzt sich detailliert mit der Entstehungsgeschichte des nunmehr vorliegenden Vorschlages auseinander und zeigt den mühsamen und langfristigen Weg der Entscheidungsprozesse in der EU deutlich auf. Hauptthema dieses Kapitels ist die Beantwortung der Frage, warum sich die Europäische Kommission für eine Verordnung und gegen eine Richtlinie entschieden hat. Begründet wird diese Entscheidung mit der langen Umsetzungsfrist einer Richtlinie sowie mit der Tatsache, dass nur eine Verordnung zu einem EU-weiten einheitlichen Datenschutz – eine solche Verpflichtung ergibt sich aus Art. 8 der Europäischen Grundrechtscharta – führen kann und darüber hinaus nur eine Verordnung eine Lösung der derzeit im grenzüberschreitenden Datenverkehr auftretenden Probleme sicherstellt.

Festgestellt wird auch, dass die Mitgliedstaaten derzeit kaum in der Lage sind, die bestehenden datenschutzrechtlichen Probleme selbst zu lösen.

3. Rechtliche Aspekte des Vorschlages

In diesem Kapitel wird auf die rechtliche Basis des Vorschlages eingegangen und detailliert begründet, warum ein Rechtsakt auf EU-Ebene notwendig ist. Weiters erfolgt eine Erklärung der einzelnen Artikel des Vorschlages auf die im vorliegenden DSG-Info-Service im

Kapitel „Allgemeine Bestimmungen“ ohnehin noch im Detail eingegangen wird, und die wir an anderer Stelle noch überblicksmäßig behandeln.

Im gegenständlichen Dokument sind insgesamt 118 Erwägungsgründe angeführt! Zweck der Erwägungsgründe ist es, die wichtigsten Bestimmungen des verfügenden Teils des Vorschlages in knapper Form zu begründen, ohne deren Wortlaut wiederzugeben.

Nachstehend folgt ein kurzer Überblick über die wichtigsten Erwägungsgründe (EWG).

Erwägungsgründe

(EWG 12) – Die Verordnung gilt nur für natürliche Personen und **nicht** für juristische Personen, wie es das österreichische DSG 2000 vorsieht.

(EWG 13) – Die Verordnung soll auch dann gelten, wenn ein EU-Auftraggeber oder EU-Dienstleister außerhalb der EU Datenverarbeitung betreibt.

(EWG 14 und 15) – Die Verordnung soll auch dann gelten, wenn ein Nicht-EU-Auftraggeber Daten verarbeitet, die EU-Bürger betreffen.

(EWG 17) – Technologieneutralität ist erklärtes Ziel der Verordnung.

(EWG 18) – Datenverarbeitung, die von der EU selbst durchgeführt wird, wird durch die vorliegende Verordnung nicht erfasst.

(EWG 19) – Datenverarbeitung für private Zwecke wird grundsätzlich nicht erfasst. Werden aber solche Daten einer unbestimmten Anzahl von Personen zugänglich, z.B. via Internet, entfällt diese Ausnahme.

(EWG 23) – Die Verordnung gilt auch für Profilerstellungen die z.B. anhand einer IP-Adresse oder der Verwendung von Cookies erfolgen.

(EWG 24) – Eine Zustimmung des Betroffenen muss ausdrücklich gegeben werden.

(EWG 27) – Personenbezogene Daten von Kindern sind besonders zu schützen. In Bezug auf die Definition „Kind“ soll die EU-Kinderrechtskonvention übernommen werden.

(EWG 28) – Die bereits in der Datenschutz-Konvention des Europarates in Art. 5 enthaltenen Qualitätsgrundsätze wie Fairness und Rechtmäßigkeit, strikte Zweckbindung, Begrenzung des Datenumfanges, Richtigkeit und Aktualität sowie zeitliche Begrenzung werden besonders betont.

(EWG 30) – Der Auftraggeber hat die Beweispflicht bezüglich der Zustimmung.

(EWG 32 – 34) – Jede Datenverarbeitung erfordert eine Rechtsgrundlage. Falls eine solche nicht identifiziert werden kann, ist eine Datenverarbeitung nur mit ausdrücklicher Zustimmung des Betroffenen zulässig.

(EWG 46 und 47) – Bei rechtswidriger Verarbeitung hat der Betroffene das „Right to be forgotten“.

(EWG 48) – Der Betroffene hat einen Anspruch auf Transfer seiner Daten von einem automatischen System in ein anderes sowie auf die Bereitstellung einer elektronischen Kopie seiner Daten.

(EWG 51) – Der Betroffene bekommt bei Vorliegen bestimmter Umstände ein Abwehrrecht gegen eine Profilerstellung eingeräumt.

Die Erstellung von Profilen von Kindern ist grundsätzlich verboten.

(EWG 55) – Falls ein Nicht-EU-Auftraggeber Daten von EU-Bürgern verarbeitet und über keine Niederlassung in einem Mitgliedstaat verfügt, so muss er einen Repräsentanten als Kontaktperson für die Aufsichtsbehörden nominieren.

(EWG 58) – Auftraggeber sind verpflichtet Data Breaches unverzüglich Aufsichtsbehörden und Betroffenen mitzuteilen. Diese Verpflichtung – bis auf die Meldepflicht – besteht im österr. DSG 2000 seit der DSG Novelle 2010 (§ 24 Abs. 2a DSG 2000).

(EWG 60) – Das generelle Meldeverfahren soll abgeschafft und durch eine schriftlich niederzulegende Risikoanalyse der jeweiligen geplanten Datenanwendung ersetzt werden.

(EWG 64) – Europäische Zertifizierungen für Produkte und Dienstleistungen sollen gefördert werden.

(EWG 79) – Datenschutzaufsichtsbehörden sollen ausreichende finanzielle und personelle Ressourcen sowie eine entsprechende Infrastruktur erhalten.

(EWG 82 und 83) – Falls sich die Datenverarbeitung über mehrere Mitgliedstaaten erstreckt, soll nur eine Datenschutzaufsichtsbehörde zuständig sein, und zwar in jenem Mitgliedstaat, wo sich die Hauptniederlassung (z.B. Konzernzentrale) befindet.

(EWG 94) – Es soll eine europäische Datenschutzbehörde gegründet werden, die aus den Vorsitzenden der einzelnen nationalen Datenschutzaufsichtsbehörden zusammengesetzt ist. Diese neue Behörde soll die Art. 29 Datenschutzgruppe ersetzen.

(EWG 97) – Die Datenschutzaufsichtsbehörden sollen das Recht des Einbringens von Verbandsklagen erhalten.

(EWG 104) – In Bezug auf die Verarbeitung von Gesundheitsdaten sollen die Verarbeitungsmöglichkeiten in den Mitgliedstaaten harmonisiert werden, um ein grenzüberschreitendes Gesundheitswesen zu ermöglichen.

(EWG 114) – Die RL 95/46/EG soll durch diese Verordnung aufgehoben werden.

Kapitel I

Allgemeine Bestimmungen

Art. 2 – Anwendungsbereich

Dieser Artikel definiert den Anwendungsbereich der Verordnung, wobei besonders Punkt 2 von Interesse ist. Dieser besagt, dass die Verordnung auch für Auftraggeber gilt, die außerhalb der EU personenbezogene Daten von EU-Bürgern verarbeiten.

Art. 3 – Definitionen

Dieser Artikel enthält insgesamt 18 Begriffsdefinitionen, wobei es vier verschiedene Definitionen für den Datenbegriff gibt, und zwar:

(2) 'personal data' means any information relating to a data subject;

(10) 'genetic data' means all data, of whatever type, concerning the hereditary characteristics of an individual;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual, and which may include: information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance; and identification of a person (healthcare professional) as provider of healthcare to the individual.

Kapitel II

Prinzipien

Art. 7 – Voraussetzungen für die Zustimmung

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance in the form of dependence between the position of the data subject and the controller.

Die Voraussetzung unter Punkt 4 ist deutlicher ausgeführt als jene des § 4 Z 12 DSG 2000.

Während nämlich das österreichische DSG 2000 als Voraussetzung für eine Zustimmung fordert, dass diese „insbesondere ohne Zwang“ abgegeben wird, fordert Punkt 4 der Verordnung, dass eine einmal abgegebene Zustimmungserklärung wirkungslos werden soll, falls ein signifikantes Ungleichgewicht zwischen Betroffenem und Auftraggeber besteht.

Kapitel III

Die Rechte des Betroffenen

Abschnitt 2

Information und Zugriff auf Daten

Art. 13 – Zugriffsrechte des Betroffenen

1. The data subject shall have the right to obtain from the controller at any time, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;

(d) the period for which the personal data will be stored;

(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object the processing of such personal data;

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(g) communication of the personal data undergoing processing and of any available information as to their source;

(h) the significance and envisaged consequences of such processing, at least in

the case of measures referred to in Article 20.

2. The data subject shall have the right to obtain from the controller a copy of the personal data undergoing processing.

Während Punkt 1 im Großen und Ganzen dem Auskunftsrecht des § 26 DSG 2000 entspricht, kann der Betroffene nach den Bestimmungen der Punkt 2 eine Kopie der über ihn verarbeiteten Daten verlangen.

Abschnitt 3

Richtigstellung und Löschung

Art. 15 – Das Recht auf vergessen werden und Löschung.

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data where:

(a) the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed; or

(b) the data subject withdraws consent on which the processing is based accordingto Article 5(1)(a), or when the storage period consented to has expired; or

(c) the data subject objects to the processing of personal data pursuant to Article 17; or

(d) their processing otherwise does not comply with this Regulation.

This right shall apply especially in relation to personal data which are made available by the data subject while he or she was a child.

2. Where the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data.

Während Punkt 1 so wie im § 27 DSG 2000 das Recht des Betroffenen auf Löschung seiner Daten enthält, sieht Punkt 2 einen sehr weit gehenden Anspruch des Betroffenen auf Löschung vor, nämlich den Anspruch an den Auftraggeber, dass dieser **alle öffentlich zugänglichen Daten**, also vor allem jene im Internet, zu löschen hat.

In Punkt 4 ist die Möglichkeit enthalten, in jenen Fällen, wo eine Löschung als nicht sinnvoll erscheint, eine Datensperrung vorzunehmen.

Art. 17 – Das Recht auf Datentransfer

1. The data subject shall have the right to object at any time to the processing of personal data which is based on points d), (e) and (f) of Article 5(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing for non-commercial purposes recognised as being in the public interest, the data subject shall have the right to object to the processing of their personal data for such marketing.

Falls die Daten des Betroffenen automationsunterstützt geführt werden, hat er nach den Bestimmungen des Punktes 1 das Recht, seine Daten in portierbarer Form zu erhalten, und zwar strukturiert und in einem Format, wel-

ches üblich ist und eine Weiterverwendung seiner Daten erlaubt. Nach den Bestimmungen des Punktes 2 hat der Betroffene überdies das Recht, seine Daten von einem System auf ein anderes System transferieren zu lassen, also z.B. von einem sozialen Netzwerk auf ein anderes.

Kapitel IV

Auftraggeber und Dienstleister

Abschnitt 1

Allgemeine Pflichten

Art. 20 – Datenschutz durch Implementierung und entsprechende Voreinstellung

Aufgrund der besonderen Risiken für die Privatsphäre und den Datenschutz wird das Prinzip des „eingebauten Datenschutzes“ gefordert. Darunter versteht man spezifische Maßnahmen, die in ein bestimmtes Produkt oder eine Technologie der Informations- und Kommunikationstechnologie integriert sein sollen, sowie die Anwendung von Datenschutz-Voreinstellungen.

Abschnitt 3

Datenschutzrisiko Abschätzung und Vorabkontrolle

Art. 30 – Datenschutzrisiko Abschätzung

1. Prior to the processing of personal data, the controller or the processor shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

2. In particular the following processing operations are likely to present such specific risks as referred to in paragraph 1:

(a) an evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's performance at work, creditworthiness, economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and likely to result in measures that produce legal effects concerning the individual or significantly affect the individual; or

(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases; or

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance); or

(d) personal data in large scale filing systems on children, genetic data or biometric data; or

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to Article 31(2)(b).

Das derzeit im DSG 2000 vorgesehene Meldeverfahren soll durch eine vom Auftraggeber oder Dienstleister durchzuführende Risikobewertung der jeweiligen Datenanwendung ersetzt werden. Diese Risikobewertung ist schriftlich niederzulegen und soll der Öffentlichkeit leicht zugänglich gemacht werden

können. Die europäische Kommission behält sich in diesem Zusammenhang vor, entsprechende Standards und Methoden für diese Risikobewertung festzulegen.

Art. 31 – Vorabkontrolle und Konsultation mit der Datenschutz Aufsichtsbehörde

In diesem Artikel wird festgelegt, unter welchen Umständen eine Vorabkontrolle oder eine Konsultation mit der Datenschutzaufsichtsbehörde notwendig ist.

Abschnitt 4

Datenschutzbeauftragter

Dieser Artikel schreibt die verpflichtende Bestellung eines betrieblichen Datenschutzbeauftragten für den Öffentlichen Bereich – unabhängig von Art und Mitarbeiteranzahl – sowie für Unternehmen ab 250 Mitarbeiter vor. Für Auftraggeber und Dienstleister, die sich schwerpunktmäßig geschäftsmäßig mit Datenverarbeitung als Geschäftsmodell auseinandersetzen, ist, unabhängig von der Mitarbeiteranzahl, ein betrieblicher Datenschutzbeauftragter zu ernennen.

Abschnitt 5

Verhaltensregeln und Zertifizierungen

Art. 36 – Zertifizierung

In diesem Artikel wird die verstärkte Förderung von EU Zertifizierungen im Bereich des Datenschutzes gefordert.

Kapitel V

Datenübermittlung in Drittstaaten oder internationale Organisationen

Art. 39 – Übermittlung mit entsprechenden Schutzmaßnahmen

1. Where the Commission has taken no decision pursuant to Article 38, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. These appropriate safeguards referred to in paragraph 1 shall be provided for by:

(a) binding corporate rules in accordance with Article 40; or

(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 56 when declared generally valid by the Commission pursuant to point (b) of Article 60(1); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 the controller or processor shall obtain prior authorisation of the contractual clauses according to Article 31(1)(a) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism set out in Article 56.

In diesem Artikel werden die notwendigen Schutzmaßnahmen erläutert, die bei einer Datenübermittlung in Drittstaaten oder zu internationalen Organisationen zu beachten sind.

Grundsätzlich wird gefordert, dass die zu treffenden Maßnahmen rechtsverbindlich sein müssen.

Art. 42 – Datenherausgabe die nicht durch EU-Recht genehmigt ist

1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.

Artikel 42 verbietet die Herausgabe von personenbezogenen Daten, die aufgrund einer Entscheidung eines Gerichtes oder einer Behörde aus einem Drittstaat gefordert wird.

Kapitel VI

Unabhängige Datenschutzbehörden

Abschnitt 1

Unabhängigkeitsstatus

Art. 46 – Unabhängigkeit

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with the duties of the office and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, cooperation and active participation in the European Data Protection Board.

6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.

7. Member States shall ensure that the supervisory authority is not subject to financial control which might affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

8. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraphs 5 to 7, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Dieser Artikel streicht die Unabhängigkeit der Datenschutzaufsichtsbehörden deutlich heraus.

Kapitel VII

Kooperation und Kohärenz

Abschnitt 1

Kooperation

Art. 55 – Gemeinsame Einsätze

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint enforcement measures and other joint operations in which designated members or staff from other Member States' supervisory authorities participate in operations within a Member State's territory.

2. In cases where data subjects in another Member State or other Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective operation and respond to the request of a supervisory authority to participate in the operations without delay.

3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorization, confer executive powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law.

Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 50(1).

6. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board

and to the Commission and shall submit the matter in the mechanism set out in Article 56.

In diesem Artikel wird die Möglichkeit gemeinsamer Einsätze der Datenschutzaufsichtsbehörden aus den verschiedenen Mitgliedstaaten beschrieben.

Abschnitt 3

Art. 63 – Die europäische Datenschutzaufsichtsbehörde

1. A European Data Protection Board is hereby set up.

2. The European Data Protection Board shall be composed of a head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Laut diesem Artikel soll eine eigene europäische Datenschutzaufsichtsbehörde gegründet werden, welche die 29er Datenschutzgruppe ersetzt.

Kapitel VIII

Rechtsmittel, Verantwortlichkeit und Sanktionen

Art. 73 Beschwerderecht an Datenschutzbehörden

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.

3. Any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State also on ist own behalf, if it considers that Articles 28 or 29 have been infringed as a result of the processing of personal data.

Dieser Artikel sieht auch die Möglichkeit einer Verbandsklage vor. Das Klagerecht bezieht sich auf unrechtmäßige Verarbeitung und gröbere Datenschutzverletzungen sowie vor allem auf Data Breaches.

Art. 79 – Verwaltungsstrafen

Dieser Artikel gibt einen Strafrahmen von mindestens EUR 100 bis max. EUR 1.000.000 vor. Bei privaten Unternehmen kann an Stelle eines Fixbetrages auch eine Verwaltungsstrafe idHv 1 % bis 5 % des jährlichen Umsatzes festgesetzt werden.

Ausblick

Sollte der vorliegende Vorschlag in Form einer Verordnung wirklich umgesetzt werden, so werden weite Teile unseres derzeitigen DSG 2000 zu ersetzen sein.

Wie vor allem die USA mit dem Ansatz der Kommission – nämlich in jedem Fall „Herr" über die Daten der EU-Bürger sein zu wollen – umgehen wird, bleibt abzuwarten.

Höhere Strafen und die Möglichkeit von Verbandsklagen könnten dazu führen, die Datenschutzstandards in Europa zu verbessern. Wie das „Right to be forgotten" in der Realität in einer vernetzten Welt funktionieren soll, ist eine offene Frage.

Es ist allerdings nicht zu erwarten, dass der vorliegende Vorschlag von den Mitgliedstaaten – immerhin bald 28 – rasch akzeptiert wird. Datenschutz-Insider gehen von mindesten 2 Jahren aus, bis die Mitgliedstaaten die Verordnung – wenn es dabei bleibt – annehmen. Und dann werden aller Wahrscheinlichkeit wieder 2 Jahre vergehen, so dass die Regelungen voraussichtlich erst in 4 Jahren in Kraft treten werden.

Wir werden Sie jedenfalls in dieser Angelegenheit auf dem Laufenden halten.

••••

Unser nächstes Seminar zum Thema

Datenschutz im modernen Unternehmen

Vom Gesetzestext bis zur unternehmenskonformen Umsetzung

findet am **17. April 2012** statt.

Es referiert der Autor des Standardwerkes zum österreichischen DSG:
KommR Hans-Jürgen Pollirer.

Die Anmeldung ist über unsere Homepage www.secur-data.at möglich.
Stärken Sie durch Ihre Teilnehme Ihre Wettbewerbsvorteile – Datenschutz gewinnt regelmäßig an Bedeutung.