RUOSS VÖGELE PARTNER
RECHTSANWÄLTE ATTORNEYS AT LAW
RVP

RUOSS VÖGELE PARTNER | KREUZSTRASSE 54 | CH-8032 ZÜRICH
TELEFON +41 44 250 43 00 | FAX +41 44 250 43 10 | info@rvpartner.ch | www.rvpartner.ch

RVP Bulletin

Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU 1/2010

Dr. Alois Rimle, LL.M.
rimle@rvpartner.ch

Zürich, März 2010, Nr. 4

Inhalt

Themen im Fokus

Geänderte EU-Standardklauseln

Die Europäische Kommission hat am 5. Februar 2010 einen Beschluss zur Änderung der Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern gefasst, um neuen Geschäftsmodellen sowie der zunehmenden Globalisierung und Auslagerung von Datenverarbeitungstätigkeiten Rechnung zu tragen. Der Beschluss enthält besondere Bestimmungen, wonach unter bestimmten Bedingungen sowie unter Wahrung des Schutzes personenbezogener Daten die *Auslagerung von Verarbeitungstätigkeiten an Unterauftragnehmer* zulässig ist.

Der Beschluss gilt ab dem 15. Mai 2010. Ein vor dem 15. Mai 2010 geschlossener Standardvertrag zwischen einem Datenexporteur und einem Datenimporteur bleibt so lange in Kraft, wie die Übermittlung und die Datenverarbeitung aufgrund dieses Vertrages unverändert weiterlaufen und von diesem Beschluss erfasste personenbezogene Daten weiterhin zwischen den Vertragsparteien übermittelt werden. Beschliessen die Vertragsparteien diesbezügliche Änderungen

oder vergeben sie einen Unterauftrag über Verarbeitungsvorgänge, die unter den Vertrag fallen, sind sie verpflichtet, einen neuen Vertrag zu schliessen, in dem die geänderten Standardvertragsklauseln berücksichtigt werden.

Die Änderung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern betrifft im Wesentlichen die Vergabe eines Unterauftrags durch den Datenimporteur. Neben einer entsprechenden Anpassung verschiedener Klauseln ist vor allem eine neue Klausel 11 eingefügt worden. Sie lautet wie folgt:

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäss Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäss Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäss Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich:

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Konzepte von "Controller" und "Processor" nach EU-Datenschutzrichtlinie

Die Artikel-29-Datenschutzgruppe hat am 16. Februar 2010 eine Stellungnahme über die Konzepte des „für die Verarbeitung Verantwortlichen" ("Data Controller") und des "Auftragsverarbeiters" ("Data Processor") veröffentlicht (Opinion 1/2010 on the concepts of "controller" and "processor" of 16 February 2010, WP 169).

Das Konzept des Data Controllers und dessen Interaktion mit dem Konzept des Data Processors spielen eine entscheidende Rolle bei der Anwendung der EU-Datenschutzrichtlinie. Sie entscheiden, wer für die Einhaltung der Datenschutzregeln verantwortlich ist, wie betroffene Personen ihre Rechte wahrnehmen können, welches das anwendbare nationale Recht ist und wie effektiv Datenschutzbehörden operieren können.

Der Data Controller ist die natürliche oder juristische Person, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die datenschutzrechtlichen Pflichten in der EU-Datenschutzrichtlinie sind im Wesentlichen an den Data Controller gerichtet. Deshalb muss bei jeder Datenbearbeitung klar sein, wer Data Controller und dementsprechend für die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich ist. Die Datenbearbeitung kann auch durch eine Mehrzahl von Data Controllern erfolgen. Andererseits ist der Data Processor die natürliche oder juristische Person, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des Data Controllers verarbeitet.

Die Artikel-29-Datenschutzgruppe anerkennt die Schwierigkeiten bei der Anwendung der Definitionen

des Data Controllers und Data Processors gemäss EU-Datenschutzrichtlinie in einem komplexen Umfeld, in dem mehrere Szenarien denkbar sind, die Controller und Processor, allein oder gemeinsam mit anderen, mit unterschiedlichen Stufen von Autonomie und Verantwortlichkeit einschliessen. Das Wesentliche bei der Qualifizierung als Data Controller oder Data Processor ist letztlich, dass die Verantwortlichkeit für die Datenbearbeitung klar definiert und zugeordnet und die praktische Einhaltung der datenschutzrechtlichen Regeln ausreichend sichergestellt werden kann.

Bei der Bestimmung des Data Controllers kommt es auf die Fähigkeit an, über die „Zwecke und Mittel der Verarbeitung von personenbezogenen Daten" zu entscheiden. Diese Fähigkeit mag auf verschiedenen rechtlichen und/oder tatsächlichen Umständen beruhen: (1) eine ausdrückliche rechtliche Befugnis, wenn das Gesetz einen Controller bezeichnet oder die Aufgabe oder Pflicht überträgt, bestimmte Daten zu sammeln und zu verarbeiten; (2) allgemeine rechtliche Bestimmungen oder bestehende traditionelle Rollen, die normalerweise bestimmte Verantwortlichkeiten innerhalb gewisser Organisationen umfassen (z.B. der Arbeitgeber in Bezug auf die Daten der Arbeitnehmer); (3) tatsächliche Umstände und andere Elemente (wie z.B. vertragliche Beziehungen, tatsächliche Kontrolle durch eine Partei, Anschein gegenüber betroffenen Personen, vernünftiges Vertrauen seitens der betroffenen Personen etc.). Wenn keiner dieser Umstände zutrifft, muss die Ernennung einer Person als Data Controller als nichtig betrachtet werden. Eine Person, die weder rechtliche noch tatsächliche Einflussmöglichkeit hat und nicht bestimmen kann, wie personenbezogene Daten zu bearbeiten sind, kann auch nicht Controller sein.

Die Funktion des Data Processors ergibt sich aus den konkreten Aktivitäten in einem bestimmten Kontext und mit Bezug auf bestimmte Datensammlungen und Abläufe. Die folgenden Kriterien mögen bei der Qualifizierung der verschiedenen Beteiligten hinsichtlich einer bestimmten Datenbearbeitung hilfreich sein: Grad der vorgängigen Instruktionen durch den Data Controller; Überwachung der Ausführung der Dienstleistungen durch den Data Controller; der durch den Data Controller erweckte Anschein gegenüber den betroffenen Personen; autonome Entscheidungsbefugnis seitens der verschiedenen Parteien.

Compliance-Check eines Videoüberwachungssystems

Die Installation einer Videoüberwachung in einem Unternehmen muss datenschutzrechtlich überprüft werden. Das gilt nicht nur für die Schweiz, sondern auch für andere Länder mit systematischen Datenschutzrechten. Die Schritte eines Compliance-Checks sollen nachfolgend nach Massgabe des schweizerischen Datenschutzrechts kurz dargestellt werden. In der Schweiz hat sich das Bundesgericht in den letzten Jahren wiederholt mit den Anforderungen an die Videoüberwachung im öffentlichen Raum befasst. Dabei hat es die entsprechende Regelung im jeweiligen kantonalen Polizeigesetz überprüft (vgl. Urteil des Bundesgerichts vom 30. September 2009, 1C-179/2008; BGE 133 I 77). Die datenschutzrechtlichen Anforderungen im öffentlichen Raum gelten grösstenteils auch für die Videoüberwachung durch Private.

Der Zweck, der mit einer Videoüberwachungsanlage verfolgt wird, ist der Angelpunkt eines datenschutzrechtlichen Compliance-Checks. Der *Zweck einer Videoüberwachungsanlage* muss detailliert festgelegt und in Richtlinien oder einem Reglement beschrieben werden. Nur wenn der angestrebte Zweck genau umschrieben wird, ist es überhaupt möglich festzustellen, ob die Videoüberwachung zulässig ist und wie sie gegebenenfalls datenschutzrechtlich umzusetzen ist. Wenn es um eine Videoüberwachung am Arbeitsplatz geht, ist der zulässige Zweck in der Schweiz eng begrenzt. Zulässig ist etwa die Videoüberwachung aus organisatorischen Gründen, aus Gründen der Sicherheit oder zur Produktionssteuerung, wobei der Arbeitnehmer dabei nicht oder nur ausnahmsweise betroffen sein darf (z.B. Videokameras ausserhalb der Gebäude und bei Parkplätzen, bei Zugängen oder Eingängen, bei gefährlichen Maschinen und Anlagen, in Tresorräumen, bei Schalterhallen einer Bank etc.). Es kann u.U. auch eine kurzzeitige, stichprobenartige Videoüberwachung der Angestellten zu Schulungszwecken zulässig sein. Nicht zulässig sind grundsätzlich Videoüberwachungssysteme, die der Überwachung des Verhaltens am Arbeitsplatz dienen. Ausnahmsweise kann gemäss einem neuen Bundesgerichtsentscheid allerdings auch eine solche Überwachung zulässig sein, wenn Arbeitnehmer nur sporadisch und kurzzeitig bei bestimmten Gelegenheiten vom Überwachungssystem erfasst werden (siehe

nachfolgende Entscheidbesprechung über die Zulässigkeit der Videoüberwachung am Arbeitsplatz).

Im Weiteren muss eine Videoüberwachung im Unternehmen datenschutzrechtlich gerechtfertigt sein (*Rechtfertigungsgrund*). Der entsprechende Eingriff in die Persönlichkeit muss mit anderen Worten durch die Zustimmung der betroffenen Personen, durch ein überwiegendes öffentliches oder privates Interesse oder durch ein Gesetz gerechtfertigt sein (Art. 13 Abs. 1 DSG). Anhand der erfolgten Zweckbestimmung ist eine spezifische Einwilligung der betroffenen Personen einzuholen bzw. zu prüfen, ob ein überwiegendes Interesse vorliegt oder sich die Rechtfertigung aus dem Gesetz ergibt.

Schliesslich ist die Videoüberwachung nur zulässig, wenn sie verhältnismässig ist (*Verhältnismässigkeitsprinzip*). Die Zweckerreichung muss geeignet und erforderlich sein. Die Videoüberwachung darf nur zur Anwendung kommen, wenn sich alternative Massnahmen (z.B. Verriegelung, Verstärkung der Eingangstür, Alarmsystem), die die Privatsphäre weniger beeinträchtigen, als ungenügend oder undurchführbar erweisen. Zudem müssen der Eingriffszweck und die Eingriffswirkung in einem vernünftigen Verhältnis stehen. Nicht jedes unerwünschte Verhalten darf mittels Videoüberwachung bekämpft werden.

Wenn einmal feststeht, dass eine beabsichtigte Videoüberwachung allenfalls mit reduziertem Zweck zulässig ist, stellt sich die Anschlussfrage, wie das Videoüberwachungssystem auszugestalten ist, damit es datenschutzkonform ist. Die *konkrete Ausgestaltung der Videoüberwachung* ist ebenfalls am (zulässigen) Zweck zu messen. Es ist anhand des besonderen Zwecks zu bestimmen, ob eine Online-Auswertung oder eine blosse Aufzeichnung der Daten erfolgen soll und ob eine 24-Stunden-Überwachung erforderlich ist oder eine Überwachung während bestimmten Zeiten genügt. Anhand des Zwecks sind auch die Verwendung der Aufzeichnungen (Zweckbindungsprinzip), der Standort der Kameras, die Aufbewahrungsdauer der Videoaufnahmen und die Zugriffsberechtigung festzulegen. Diese und andere Aspekte der Datenbearbeitung (z.B. Verantwortlichkeiten, erfasste Bereiche und Personen, Sicherheitsmassnahmen zum Schutz vor unbefugter Bearbeitung) sind wie die Zweckbestimmung in Richtlinien oder einem Reglement zu beschreiben.

Die Verantwortlichen der Videoüberwachung müssen gemäss EDÖB die Personen, die das Aufnahmefeld der Kameras betreten, grundsätzlich mit einem gut sichtbaren Hinweisschild über das Überwachungssystem informieren. Wenn die aufgenommenen Bilder mit einer Datensammlung verbunden sind, muss auch angegeben werden, bei wem das Auskunftsrecht geltend gemacht werden kann, es sei denn, dies ergibt sich aus den Umständen.

In diesem Zusammenhang soll kurz rechtsvergleichend auf die gesetzliche Regelung der Videoüberwachung in Deutschland hingewiesen werden. Das Thema ist aufgrund der Abhörskandale in den Grossunternehmen Lidl, Telekom und Bahn auch in Deutschland sehr aktuell. Das Bundesdatenschutzgesetz sieht eine Regelung für die Videoüberwachung (§ 6b) nur für öffentlich zugängliche Räume vor (z.B. Tankstellen). Im Übrigen ist eine generelle Zulässigkeitsprüfung (§ 4 Abs. 1 BDSG) erforderlich. Im Weiteren sind andere Rechtsnormen zu berücksichtigen, insbesondere kollektive Regelungen über die Verhaltens- und Leistungskontrolle der Beschäftigten (§ 87 Abs. 1 Nr. 6 BetrVG).

Zulässigkeit der Videoüberwachung am Arbeitsplatz (Entscheid)

Das schweizerische Bundesgericht hatte vor kurzem die Videoüberwachung des Kassenraums eines Unternehmens zu beurteilen. Es stellte insbesondere fest, dass die Videoüberwachung im vorliegenden Fall sowohl aus Sicht des öffentlichen Arbeitsrechts als auch aus Sicht des Persönlichkeits- und Datenschutzrechts zulässig sei (Urteil des Bundesgerichts vom 12. November 2009, 6B-536/2009).

Art. 26 der Verordnung 3 zum Arbeitsgesetz hält u.a. fest, dass Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden dürfen. Diese Verordnungsbestimmung ist gemäss Bundesgericht so nicht haltbar und gesetzeswidrig. Eine (hauptsächlich) der Überwachung des Verhaltens der Arbeitnehmer am Arbeitsplatz dienende Massnahme beeinträchtige nicht eo ipso die Gesundheit der Arbeitnehmer. Sie sei deshalb nicht in jedem Fall zu verbieten. Ein Überwachungssystem könne daher, auch wenn es (hauptsächlich) der gezielten Überwachung des Verhaltens der Arbeitnehmer am Arbeitsplatz diene, erlaubt sein, wenn die Arbeitnehmer *nur*

sporadisch und kurzzeitig bei bestimmten Gelegenheiten vom Überwachungssystem erfasst würden. Im vorliegenden Fall halten sich die Arbeitnehmer gemäss Feststellung des Gerichts nur sporadisch und während kurzer Zeit im Kassenraum auf, namentlich um dort Bargeld zu deponieren oder zu holen. Dabei werde das Verhalten der Arbeitnehmer nicht über längere Zeit überwacht. Eine solche Videoüberwachung sei nicht geeignet, die Gesundheit und das Wohlbefinden der Arbeitnehmer zu beeinträchtigen. Sie sei mangels Relevanz unter dem Gesichtspunkt der Gesundheit und des Wohlbefindens der Arbeitnehmer zulässig.

Die Videoüberwachung im Kassenraum ist gemäss Bundesgericht auch unter den Gesichtspunkten des Persönlichkeitsschutzes und des Datenschutzes nicht rechtswidrig. Die Persönlichkeit der Arbeitnehmer werde im Sinne von Art. 28 ZGB, Art. 328 und Art. 328b OR bzw. Art. 12 DSG nicht widerrechtlich verletzt. Die Videoüberwachung des Kassenraums bezwecke nicht ausschliesslich die Überwachung des Personals, sondern auch die Verhinderung von Straftaten durch Dritte. Im Kassenraum eines Uhren- und Juwelengeschäfts können sich gemäss Bundesgericht Bargeldbeträge in beträchtlichem Umfang befinden. Deshalb habe der Geschäftsinhaber ein erhebliches Interesse an einer Überwachung. Zudem würden die Arbeitnehmer im Verlauf eines Arbeitstages nur sporadisch und kurzzeitig erfasst. Die Zulässigkeit der Videoüberwachung sei im vorliegenden Fall auch gegeben, wenn die betroffenen Arbeitnehmer weder wussten noch mit der Möglichkeit rechneten, dass auch im Kassenraum eine Videokamera installiert und während den Geschäftszeiten in Betrieb sein könnte.

Bearbeitung von Kreditdaten (Stellungnahme)

Die Artikel-29-Arbeitsgruppe hat am 1. Dezember 2009 zum Bericht der Expertengruppe “Kredithistorien“ Stellung genommen (Beitrag der Artikel-29-Arbeitsgruppe zur öffentlichen Konsultation der GD MARKT zu dem Bericht der Expertengruppe “Kredithistorien“ vom 1. Dezember 2009, WP 164). Die Expertengruppe “Kredithistorien“ ist von der Europäischen Kommission beauftragt worden, Lösungen zur Optimierung der Weiterleitung von Kreditdaten innerhalb der EU zu erarbeiten. Der Bericht der Expertenkommission befürwortet eine weitere Liberalisierung. Diesbezüglich weist die Artikel-29-Arbeitsgruppe in ihrem Beitrag in Anwendung der EU-Datenschutzrichtlinie auf verschiedene datenschutzrechtliche Aspekte hin, insbesondere die Folgenden:

- Ein vollumfängliches Informationsrecht ist das wichtigste Recht für die betroffenen Personen. Die betroffenen Personen müssen über jeden sie betreffenden Eintrag im Kreditregister informiert werden. Die betroffenen Personen müssen wissen, an wen sie sich im Fall eines Streits oder im Fall von Anfragen in Bezug auf die Verarbeitung ihrer Personendaten in Kreditregistern wenden müssen. Der für die Verarbeitung der Daten in Kreditregistern Verantwortliche oder sein Vertreter muss angegeben werden. Bei Vertragsabschluss sollte die betroffene Person darüber informiert werden, dass ihre Kreditdaten zur Bewertung ihrer Zahlungsfähigkeit eingesehen und dass ihre Finanzdaten in eine Negativdatei aufgenommen werden könnten, sollten sie ihren finanziellen Verpflichtungen nicht nachkommen.
- Das Auskunfts- und das Berichtigungsrecht müssen gegen jede Kreditauskunftsstelle durchsetzbar sein, die Kreditdaten erhalten hat.
- Die personenbezogenen Daten, die in Kreditregistern verarbeitet werden dürfen, müssen definiert werden. Es dürfen keine personenbezogene Daten über den angestrebten Zweck hinaus verarbeitet werden.
- Es ist zu unterscheiden zwischen Informationsverzeichnissen über Zahlungsunfähigkeit und Kreditwürdigkeit einerseits und Informationen über die Nichteinhaltung von finanziellen Verpflichtungen andererseits (vgl. Arbeitspapier über Schwarze Listen, WP 65). Für Negativdateien, die Informationen über die Nichteinhaltung von finanziellen Verpflichtungen enthalten, ist die Zustimmung der betroffenen Person nicht erforderlich. Für die Erhebung von Informationen über die Zahlungsunfähigkeit ist die Zustimmung hingegen erforderlich.
- Mechanismen zur Kontrolle der Datenqualität sind im Bereich der Verarbeitung von Kreditdaten wesentlich. Es muss sichergestellt werden, dass die Daten des Kreditnehmers keine fehlerhaften, sachlich unrichtigen oder unerheblichen Informationen enthalten.
- Es dürfen ausschliesslich die unbedingt erforderlichen Daten an die Kreditgeber weitergegeben

werden (Grundsatz der Zweckbindung und Verhältnismässigkeit).

- Der grenzüberschreitende Zugang der Kreditgeber zu den Kreditdaten und deren weitere Verarbeitung müssen sowohl dem Datenschutzgesetz des Kreditinstituts als auch jenem der Kreditauskunftsstelle entsprechen.
- Die Kreditdaten dürfen nur so lange wie es erforderlich und angemessen ist und im Einklang mit den innerstaatlichen Vorschriften aufbewahrt werden. Eine unbegrenzte Speicherung solcher Daten für Kreditzwecke oder für in keinem Zusammenhang mit der Speicherung stehende Zwecke ist untersagt. Die Artikel-29-Arbeitsgruppe spricht sich gegen die Möglichkeit für Kreditgeber aus, während der gesamten Laufzeit eines Kredits und darüber hinaus Zugang zu den Kreditdaten zu haben.

Datenweitergabe durch Kreditauskunftsstelle (Entscheid)

Das schweizerische Bundesverwaltungsgericht hatte sich vor Kurzem mit der Weitergabe von Personendaten durch eine Kreditauskunftsstelle (Kreditauskunftei) zu befassen. Eine Kreditauskunftsstelle bot Arbeitgebern die Möglichkeit an, über potentielle Arbeitnehmer umfassende Bonitätsauskünfte sowie weitgehende Informationen über deren persönliches Umfeld einzuholen.

Das Bundesverwaltungsgericht führt in seinem Entscheid u.a. aus, eine Weitergabe solcher Daten an (potentielle) Arbeitgeber könne und müsse von den betroffenen Personen nicht erwartet werden und sei damit treuwidrig. Die im Rahmen des “Mitarbeiter-Checks“ weitergegebenen Daten erscheinen gemäss Gericht zudem für die Beurteilung der Eignung von Mitarbeitenden in der Regel weder geeignet noch erforderlich. Die Datenbekanntgabe sei damit unverhältnismässig. Ein Rechtfertigungsgrund für die Weitergabe der Daten sei nicht ersichtlich und auch nicht geltend gemacht worden. Im Ergebnis erscheine nicht erst die Verwendung der Daten im Rahmen eines Arbeitsverhältnisses, sondern bereits deren Weitergabe an Dritte als widerrechtlich (Entscheid des Bundesverwaltungsgerichts vom 14. Januar 2009, Nr. A-8028/2008).

Die Zukunft des Datenschutzes (Stellungnahme)

Am 9. Juli 2009 hat die Europäische Kommission ein Konsultationsverfahren zum Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, die sich insbesondere aus den neuen Technologien und der Globalisierung ergeben.

Zu diesem Konsultationsverfahren haben die Artikel-29-Arbeitsgruppe und die Arbeitsgruppe Polizei und Justiz am 1. Dezember 2009 eine gemeinsame Stellungnahme verabschiedet. Es wird darin festgestellt, dass die wichtigsten Grundsätze des Datenschutzes trotz der neuen Technologien und der Globalisierung nach wie vor gültig seien, dies aber nicht bedeute, dass keine Gesetzesänderungen erforderlich seien. Die gemeinsame Stellungnahme enthält im Wesentlichen folgende Vorschläge:

- Einführung eines umfassenden Rechtsrahmens auf Stufe EU, der durch spezielle Gesetze in gewissen Sektoren und durch innerstaatliche Verordnungen ergänzt werden kann (Architektur eines umfassenden Rechtsrahmens);
- Entwicklung internationaler globaler Normen, falls möglich in Form eines bindenden internationalen Rechtsrahmens (Verweis auf Madrid-Resolution);
- Erlass von verbindlichen unternehmensinternen Datenschutzregeln (Weiterentwicklung der BCRs) sowie Einführung einer Rechenschaftspflicht für multinationale Unternehmen;
- Berücksichtigung des Datenschutzes bei der Planung von Informations- und Kommunikationstechnologien (Grundsatz „Privacy by Design“);
- Stärkung der Position der betroffenen Personen; Stärkung der Verantwortung der für die Datenverarbeitung Verantwortlichen; Stärkung der Rolle der nationalen Datenschutzbehörden.

Weitere Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz

Der betriebliche Datenschutzverantwortliche

Der EDÖB hat in einer Mitteilung vom 11. März 2010 die Möglichkeit der datenschutzrechtlichen Selbstregulierung gemäss dem revidierten Datenschutzgesetz erläutert. Wenn ein Unternehmen einen Datenschutzverantwortlichen ernennt und den EDÖB darüber informiert, darf es darauf verzichten, ihre Datensammlungen beim EDÖB anzumelden.

Allerdings müssen Position und Person des Datenschutzverantwortlichen gewisse Kriterien erfüllen. Der EDÖB gibt insbesondere folgende Empfehlungen ab, wie die datenschutzrechtliche Selbstregulierung innerhalb des Unternehmens organisiert werden könnte:

- *Datenschutzmanager:* Ernennung von Datenschutzmanagern in unteren Hierarchiestufen, die einen Teil ihrer Arbeitszeit für den Datenschutz in ihrem Bereich einsetzen und die Kommunikation zwischen dem betrieblichen Datenschutzverantwortlichen und den einzelnen Abteilungen oder Bereichen gewährleisten;
- *Meldung und Kontrolle von Datensammlungen (Datenschutzprozess):* Einführung einer internen Meldepflicht zwecks Überwachung, wonach mit einem standardisierten Formular vorhandene und geplante Datensammlungen und Datenbearbeitungen gemeldet werden;
- *Risikobeurteilung (Datenschutzprozess):* Durchführung von Risikoanalysen aufgrund der gemeldeten Datensammlungen und Datenbearbeitungen;
- *Meldung von Datenschutzverletzungen (Datenschutzprozess):* Sicherstellung des Informationsflusses zwischen der betroffenen Abteilung und dem betrieblichen Datenschutzverantwortlichen im Fall einer Datenschutzverletzung zwecks Risikominimierung und Umsetzung von Notfallszenarien.
- *Datenschutz-Informationsseite:* Erstellung einer Informationsseite zum Thema Datenschutz auf dem Intranet, auf der sämtliche relevanten Dokumente zur Verfügung gestellt werden.

Datenweitergabe bei Unternehmenszusammenschlüssen

Der EDÖB hat in einer Mitteilung von Anfang März 2010 auf verschiedene Risiken bei der Datenweitergabe im Rahmen von Unternehmenszusammenschlüssen hingewiesen. Gemäss Mitteilung müssen die datenschutzrechtlichen Risiken bei Fusionen und Unternehmenskäufen analysiert und ausreichend berücksichtigt werden. Es werden insbesondere folgende Empfehlungen abgegeben:

- Abschluss von Non Disclosure Agreements mit datenschutzrechtlichen Klauseln vor einer Due Diligence (Regelung der Datenrückgabe bzw. Datenvernichtung, Beschränkung der Datenverwendung etc.);
- Beschränkung des Umfangs der Datenoffenlegung nach Massgabe des jeweiligen Verfahrensstadiums;
- Anonymisierung der Personendaten soweit praktikabel;
- Beachtung gesetzlicher und vertraglicher Geheimhaltungspflichten;
- Prüfung vor dem Closing, ob der bei der Datenerhebung angegebene Zweck mit der geplanten zukünftigen Datenbearbeitung im Einklang steht; allenfalls Information der betroffenen Personen und falls erforderlich Einholung der Zustimmung.

Zugangskontrolle (Entscheid)

Das Bundesverwaltungsgericht hatte sich im Jahre 2009 mit einem Zugangskontrollsystem zu befassen (Urteil des Bundesverwaltungsgerichts vom 4. August 2009, A-3908/2008). Die KKS Sport- und Freizeitanlagen Schaffhausen (KSS) führte im Sommer 2005 zum Zweck der Missbrauchsbekämpfung bei der Benutzung persönlicher, nicht übertragbarer Jahres- und Halbjahresabonnemente für den Eintritt ins Hallenbad und den Wellness-Bereich ein neues Zugangskontrollsystem ein. Im Rahmen des neuen Systems werden von den Kunden neben den Personalien auch digital komprimierte bzw. reduzierte Darstellungen eines biometrischen Abdrucks, im vorliegenden Fall des Fingerabdrucks, sogenannte Templates, erhoben. Der Fingerabdruck wird analysiert und die Merkmale des Abbilds (Anfangs- und Endpunkte, Gabelungen etc.), “Minutien“ genannt, werden extrahiert. Die Minutien-Daten (insgesamt 20-50) sind für

jeden Menschen einzigartig. Im Weiteren erhält der Kunde eine Transponderkarte in Kreditkartenformat mit einer einmaligen Karten-ID. Die Personalien des Kunden und das Templates werden dieser Karten-ID zugeordnet. Auf der Karte sind keine Daten gespeichert. Sie ist lediglich mit einem Unterschriftsfeld versehen, damit sie optisch unterschieden werden kann. Um Zugang zum Hallenbad der KSS zu erhalten, hat der Kunde seine Transponderkarte in ein Lesegerät am Drehkreuz zu schieben und seinen Finger auf einen Scanner zu legen. Über die individuelle Karten-ID wird aus der zentralen Datenbank das entsprechende Template abgerufen und mit dem Fingerabdruck des Kunden verglichen. Es handelt sich dabei um einen Verifizierungsprozess. Bei diesem Vorgang werden das Datum, die Uhrzeit und der Kontrollautomat des Ein- bzw. Austritts erfasst.

Das Bundesverwaltungsgericht stellt in seinem Entscheid zunächst fest, dass sämtliche in Frage stehenden Daten als *Personendaten* zu qualifizieren seien und eine Bearbeitung von Personendaten gemäss Datenschutzgesetz vorliege. Insbesondere seien der Fingerabdruck wie auch die extrahierten Minutien einzigartig und nur einer bestimmten Person zuzuordnen. Mit einer zentral abgelegten Zuordnungsliste sei der Rückschluss auf einen bestimmten Abonnenten möglich.

Im Weiteren wird im Entscheid eine *Verhältnismässigkeitsprüfung* vorgenommen. Nach Art. 4 Abs. 2 DSG muss die Bearbeitung der Daten verhältnismässig sein. Sowohl der Zweck als auch die Art und Weise der Bearbeitung müssen verhältnismässig sein. Verlangt wird zunächst, dass Personendaten nur soweit bearbeitet werden, als dies für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich ist. Verlangt wird weiter, dass die Datenbearbeitung für die betroffene Person sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel zumutbar ist. Aus der Erforderlichkeit ergibt sich, dass eine Massnahme zu unterbleiben hat, wenn eine ebenfalls geeignete, aber mildere Massnahme für den angestrebten Erfolg ausreichen würde. Im vorliegenden Fall vergleicht das Gericht das aktuelle System mit einem alternativen System, das vom EDÖB vorgeschlagen wird. Während beim aktuellen System die biometrischen Daten zusammen mit einer Zuordnungsliste auf dem Host der KKS gespeichert werden, erfolgt bei dem vom EDÖB empfohlenen System „Smartcard match on card“ der Vergleich zwischen der biometrischen Charakteristik (Fingerabdruck) und den lokal gespeicherten biometrischen Daten (Referenz-Template) dezentral auf der Karte, so dass der Host lediglich ein Freigabesignal von der Smartcard erhält und keine biometrischen Daten zwischen Smartcard und dem elektronischen Zugangskontrollsystem ausgetauscht werden. Dabei haben die betroffenen Personen sowohl die Kontrolle über ihre biometrischen Referenzdaten als auch über die Transaktionsdaten im Rahmen des Vergleichs. Lediglich Transaktionsdaten, die zwischen der Smartcard und dem Leser ausgetauscht werden, liegen ausserhalb des Kontrollbereichs der betroffenen Person. Bei der Gegenüberstellung der beiden verschiedenen Zugangssystemen wird gemäss Gericht ersichtlich, dass das vom EDÖB vorgeschlagene System weit weniger in das informationelle Selbstbestimmungsrecht der betroffenen Person eingreift als das bis anhin verwendete System und trotzdem das verfolgte Ziel erreichen kann. Die betroffene Person gibt ihre Daten nicht mehr aus der Hand und behält dabei stets die Kontrolle. Es ergibt sich aus dem Vergleich der beiden Systeme, dass die zentrale Speicherung der biometrischen Daten dem Gebot der Erforderlichkeit und mithin dem Grundsatz der Verhältnismässigkeit widerspricht. Es liegt eine Persönlichkeitsverletzung nach Art. 12 Abs. 2 lit. a DSG vor.

Nicht jede Verletzung der Persönlichkeit ist widerrechtlich. Sie ist u.a. dann nicht widerrechtlich, wenn sie *durch Einwilligung des Verletzten gerechtfertigt* ist (Art. 13 Abs. 1 DSG). Eine gültige Einwilligung setzt voraus, dass sie nach angemessener Information freiwillig erfolgt (Art. 4 Abs. 5 DSG). Eine Einwilligung gilt in der Lehre dann als freiwillig, wenn der betroffenen Person eine Handlungsalternative zur Verfügung steht, die nicht mit unzumutbaren Nachteilen behaftet ist, oder die Einwilligung mindestens subjektiv im Interesse der betroffenen Person liegt. Im vorliegenden Fall verneint das Gericht u.a. die Freiwilligkeit und mithin die gültige Einwilligung, weil einerseits dem Kunde (faktisch) keine Alternativmöglichkeit geboten werde und andererseits die Einwilligung diesem keinen Vorteil bringe.

Eine Verletzung der Persönlichkeit ist ebenfalls nicht widerrechtlich, wenn sie *durch ein überwiegendes privates Interesse gerechtfertigt* ist (Art. 13 Abs. 1 DSG). Im vorliegenden Fall verneint das Gericht ein

überwiegendes Interesse der KKS an der betreffenden Datenbearbeitung. Das Interesse der KKS beziehe sich nicht auf die Datenbearbeitung, sondern betreffe lediglich die Unannehmlichkeiten, die eine Änderung der Zugangskontrolle mit sich bringen würde. Derartige Interessen könnten nicht berücksichtigt werden. Ein überwiegendes privates Interesse der KKS sei zu verneinen.

Im Ergebnis hat die KKS mit dem bisherigen Zugangssystem und der entsprechenden Art und Weise der Bearbeitung der biometrischen Daten den Grundsatz der Verhältnismässigkeit verletzt. Diese Verletzung ist weder durch Einwilligung noch durch überwiegendes privates Interesse gerechtfertigt.

Datenschutzzertifizierung von Produkten

Gemäss Art. 5 Abs. 1 VDSZ sind Produkte zertifizierbar, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten, namentlich Daten über den Benutzer, generiert werden. Art. 5 Abs. 3 VDSZ sieht vor, dass der EDÖB bis spätestens am 1. Januar 2010 Richtlinien darüber erlässt, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind.

Die genannte Frist konnte vom EDÖB nicht eingehalten werden; es ist ein Antrag an den Bundesrat gestellt worden, die Frist in Art. 5 Abs. 3 VDSZ zu streichen. Bei der Erstellung der Richtlinien haben sich verschiedene Probleme ergeben, die vertiefte Abklärungen erforderlich machen. Es wird zunächst eine Arbeitsgruppe eingesetzt, um Lösungen zu den gestellten Problemen zu erarbeiten. Anschliessend sollen entsprechende Richtlinien mit oder ohne Änderung der Datenschutzzertifizierungsverordnung erlassen werden.

Einholung von Gutachten durch Haftpflichtversicherer

Der EDÖB hat Ende 2009 die datenschutzrechtlichen Anforderungen an das Einholen von Gutachten durch Haftpflichtversicherer in Erinnerung gerufen (siehe Website des EDÖB). Haftpflichtversicherer holen regelmässig Gutachten bei externen Experten (Ärzten, Ingenieuren, Biomechaniker, Betriebswirtschaftern etc.) ein. Diese dienen den Versicherern als Grundlage zur Abklärung ihrer Leistungspflicht. Dabei müssen gemäss EDÖB die Regeln des datenschutzrechtlichen Outsourcings gemäss Art. 10a DSG beachtet werden. Im Weiteren greift die Informationspflicht nach Art. 7a DSG ein, wenn dem Gutachter Gesundheitsdaten weitergeleitet werden. Der Haftpflichtversicherer muss die betroffenen Personen in solchen Fällen darüber informieren, dass ihre Personendaten für das Erstellen eines Gutachtens auch an einen externen Gutachter übergeben werden können (Art. 7a Abs. 2 lit. c DSG). Die Information erfolgt in der Regel bereits bei der Erhebung der Personendaten durch den Haftpflichtversicherer, spätestens aber zum Zeitpunkt der Übergabe der Personendaten an den externen Gutachter.

Vorsorgliche Massnahmen (Entscheid)

Das Bundesverwaltungsgericht hatte im Zusammenhang mit der Weitergabe von Daten durch eine Kreditauskunftsstelle einen Antrag des EDÖB auf Anordnung vorsorglicher Massnahmen zu prüfen (Entscheid des Bundesverwaltungsgerichts vom 14. Januar 2009, Nr. A-8028/2008). Gemäss Art. 33 Abs. 2 DSG kann der EDÖB dem Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen, wenn er bei einer Sachverhaltsabklärung nach Art. 29 Abs. 1 DSG feststellt, dass den betroffenen Personen ein nicht leicht wieder gutzumachender Nachteil droht.

Das Massnahmenverfahren gemäss Art. 33 Abs. 2 DSG folgt verfahrensrechtlich zivilprozessualen Grundsätzen, ist aber inhaltlich öffentlich-rechtlicher Natur. Die für den Erlass von vorsorglichen Massnahmen in der Verwaltungsrechtspflege entwickelten Grundsätze können gemäss Bundesverwaltungsgericht daher auf das Verfahren gemäss Datenschutzgesetz angewendet werden, soweit nicht dessen besondere Natur ein Abweichen verlangt.

Bei der Beurteilung beantragter vorsorglicher Massnahmen nimmt das Gericht folgende Prüfungsschritte vor:

- Es ist (obwohl gesetzlich nicht ausdrücklich vorgesehen) im Sinne einer Hauptsachenprognose zunächst zu prüfen, ob die Voraussetzungen einer Sachverhaltsabklärung gemäss Art. 29 Abs. 1 DSG gegeben sind und zu erwarten ist, dass der Gesuchsteller eine Änderung der Datenbearbeitung – sei es mit einer Empfehlung oder mittels

Klage vor dem Bundesverwaltungsgericht – durchsetzen wird.

- Es ist in einem weiteren Schritt zu prüfen, ob den betroffenen Personen ein nicht leicht wieder gutzumachender Nachteil droht. Dabei ist der drohende Nachteil für die betroffenen Personen den Nachteilen gegenüberzustellen, die der Gesuchsgegnerin aus der Anordnung vorsorglicher Massnahmen erwachsen.
- Es ist schliesslich zu prüfen, ob die Anordnung einer vorsorglichen Massnahme verhältnismässig erscheint. Weil eine Empfehlung des EDÖB erst nach durchgeführter Sachverhaltsabklärung erlassen werden kann, kann es angemessen erscheinen, für die Dauer der Abklärungen und bis zu einem allfälligen Entscheid des Gerichts vorsorgliche Massnahmen anzuordnen.

Institutionelle Stellung des EDÖB

Der Bundesrat hat im September 2009 eine Botschaft und einen Gesetzesentwurf zur Umsetzung der Schengener Weiterentwicklung im Bereich des Datenschutzes verabschiedet. Der Gesetzesentwurf setzt den entsprechenden EU-Rahmenbeschluss um, soweit die schweizerische Gesetzgebung dessen Anforderungen nicht bereits vollständig erfüllt.

Die geplante Änderung des Datenschutzgesetzes, die bereits Ende 2010 in Kraft treten soll, sieht neben verschiedenen Pflichten der Bundesorgane auch eine Neuregelung der institutionellen Stellung des EDÖB vor. Die Gesetzesänderung soll die Unabhängigkeit des Datenschutzbeauftragten gewährleisten. Die Wahl des Datenschutzbeauftragten durch den Bundesrat muss neu durch das Parlament genehmigt werden. Der Datenschutzbeauftragte wird für vier Jahre gewählt. Danach wird die Amtsdauer jeweils stillschweigend um vier weitere Jahre verlängert. Die Entlöhnung des Datenschutzbeauftragten hängt nicht von einer Leistungsbeurteilung ab. Der Bundesrat kann nur aus sachlich hinreichenden Gründen eine Nichtwiederwahl verfügen. Eine Amtsenthebung ist nur möglich, wenn der Datenschutzbeauftragte seine Amtspflichten vorsätzlich oder grobfahrlässig verletzt hat oder nicht mehr fähig ist, sein Amt weiter auszuüben. Ein entsprechender Entscheid kann beim Bundesverwaltungsgericht angefochten werden.

Weitere Entwicklungen im Unternehmens-Datenschutzrecht der EU

EU-US-Abkommen zu SWIFT

SWIFT ist ein internationales Zahlungsverkehrssystem. Es handelt sich um ein Gemeinschaftsunternehmen der Finanzbranche mit Sitz in Belgien. Weltweit vollzieht SWIFT täglich 15 Millionen Überweisungen. Es sind über 8000 Banken am System angehängt. Die Transaktionsdaten enthalten nebst Betrag auch den Namen, die Adresse, die Kontonummer sowie den Banknamen sowohl vom Absender als auch vom Empfänger.

Die EU und die USA haben 2009 ein Abkommen abgeschlossen, wonach die US-Behörden zwecks Terrorismusbekämpfung Zugang zu Daten europäischer Banküberweisungen erhalten. Ein formelles Abkommen mit der EU wurde aus US-Sicht nötig, weil europäische Transaktionen ab Anfang 2010 nicht mehr zusätzlich in einem US-Datenzentrum gespeichert werden. Sie werden neu nur noch in den Niederlanden und in einem neuen Zentrum in der Schweiz gespeichert.

Dieses Abkommen betrifft indirekt auch die Schweiz. US-Fahnder haben auch Zugang zu Daten von Überweisungen ab Schweizer Bankkonten, weil die Daten von innereuropäischen Überweisungen nicht nur in der Schweiz, sondern auch im niederländischen Datenzentrum und damit im EU-Raum gespeichert werden.

Erfahrungen mit BCRs und Vergleich mit vertraglicher Lösung

Binding Corporate Rules ("BCRs") sollen innerhalb einer internationalen Unternehmensgruppe, die über die Mitgliedstaaten der EU und des EWR hinausreichen, ein angemessenes Schutzniveau im Sinne von Art. 25 DSRL schaffen, um einen ungehinderten Datenfluss innerhalb des Unternehmensverbundes zu ermöglichen. Die BCRs als solche sind in der EU-Datenschutzrichtlinie nicht ausdrücklich vorgesehen. Sie wurden von der Artikel-29-Datenschutzgruppe entwickelt.

Im Jahre 2008 hat die Artikel-29-Datenschutzgruppe detaillierte inhaltliche und formale Vorgaben für BCRs verabschiedet. Inhaltlich enthalten BCRs insbesonde-

re ein weitgehendes Haftungsregime und ein Compliance-System, mit dem die unternehmensübergreifende Befolgung der datenschutzrechtlichen Regeln sichergestellt werden soll. BCRs müssen grundsätzlich von den Datenschutzbehörden der betroffenen Mitgliedstaaten genehmigt werden. Es bestehen gegenwärtig unterschiedliche Antragsvoraussetzungen und Antragsverfahren. Eine Datenschutzbehörde übernimmt die Federführung hinsichtlich der Abstimmung der verschiedenen Genehmigungsverfahren ("Lead Authority"). Die Einholung unterschiedlicher Genehmigungen kann erfahrungsgemäss mehrere Jahre in Anspruch nehmen. Um hier Abhilfe zu schaffen, sind inzwischen 13 EU-Staaten und drei EWR-Staaten einer Vereinbarung beigetreten, wonach die jeweiligen Genehmigungen der anderen Mitgliedstaaten auf Gegenseitigkeitsbasis anerkannt werden. Allerdings fehlt es noch an einer rechtlichen Absicherung für eine solche „mutual recognition". Bislang ist lediglich eine geringe Anzahl von BCRs genehmigt worden. Sie werden von internationalen Konzernen aufgrund der umfangreichen inhaltlichen und formellen Anforderungen als unattraktiv und zu aufwendig empfunden.

Vor diesem Hintergrund erscheint gegenwärtig die Verwendung der in der EU-Datenschutzrichtlinie vorgesehenen Standardvertragsklauseln (Art. 26 Abs. 2) im konzerninternen Verhältnis bedeutend einfacher zu sein. Standardvertragsklauseln, die in einem oder mehreren multilateralen Verträgen zwischen betroffenen Gruppengesellschaften integriert werden, schaffen ein angemessenes Schutzniveau und ermöglichen den ungehinderten Datenfluss innerhalb des Unternehmensverbundes. Auf diese Weise kann im Konzern auch ohne behördliche Genehmigung sichergestellt werden, dass den Garantieanforderungen in den relevanten Mitgliedstaaten der EU und des EWR entsprochen wird (siehe ausführlich RVP Datenschutz-Bulletin 1/2009).

Suchmaschine von Google

Die Artikel-29-Datenschutzgruppe publizierte am 4. April 2008 die Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148). Google nahm auf der Grundlage dieser Stellungnahme verschiedene datenschutzrechtliche Verbesserungen vor. Die Artikel-29-Datenschutzgruppe hat diese Anstrengungen anerkannt, weist Google aber in einem öffentlichen Schreiben vom 23. Oktober 2009 auf folgende verbleibende Punkte hin, die einer Klärung bedürften:

Google hat die Aufbewahrungsdauer von Daten (vor der Anonymisierung) von 18 auf 9 Monate reduziert. Die Artikel-29-Datenschutzgruppe ist in ihrem Schreiben vom 23. Oktober 2009 der Auffassung, dass die Aufbewahrungsdauer angesichts des Bearbeitungszwecks der Suchmaschinen auf 6 Monate reduziert werden sollte.

Gemäss Stellungnahme vom 4. April 2008 (WP 148) kommt als Alternative zur Löschung die Anonymisierung in Frage. Die Anonymisierung muss aber vollständig unumkehrbar sein. Dies kann gemäss Stellungnahme die Beseitigung von Teilen der Suchhistorie erfordern, um die Möglichkeit einer indirekten Identifizierung des Benutzers auszuschliessen, der die Suchvorgänge durchgeführt hat. Im Schreiben vom 23. Oktober 2009 führt die Artikel-29-Datenschutzgruppe aus, die gegenwärtig von Google verwendete Methode (Löschung der letzten Achtergruppe der IP Adresse) stelle keine vollständige Anonymisierung dar. Es seien andere technische Möglichkeiten zu prüfen, um eine vollständige Anonymisierung zu erreichen.

Wenn die Suchmaschinenbetreiber einen Cache-Speicher bereitstellen, in dem personenbezogene Daten länger als in der ursprünglichen Veröffentlichung verfügbar gemacht werden, müssen sie das Recht der betroffenen Personen respektieren, über den Zweck hinausgehende und unrichtige Daten aus dem Cache-Speicher entfernen zu lassen. Im Schreiben vom 23. Oktober 2009 weist die Artikel-29-Datenschutzgruppe auf die Verantwortung von Google als für die Verarbeitung Verantwortlicher hin. Sobald Daten auf den Websites entfernt oder geändert worden seien, werde Google Verantwortlicher bezüglich der (veralteten) Personendaten, die im Index oder Cache-Speicher enthalten seien. Die Artikel-29-Datenschutzgruppe weist auf die beschränkte Kapazität des Google URL Removal Tool hin. In einigen Fällen habe es Wochen oder gar Monate gedauert, bis die Suchergebnisse die Aktualisierungen der Website reflektiert hätten. Deshalb ist nach Auffassung der Artikel-29-Datenschutzgruppe das Removal Tool technisch zu verbessern, damit Endbenutzer sensible Informationen wirklich von den Suchergeb-

nissen entfernen können, sobald die Original-Website geändert worden ist.

Änderung des BDSG in Deutschland

Am 1. September 2009 sind wichtige Änderungen des Bundesdatenschutzgesetzes in Kraft getreten. Für weitere Änderungen gelten Übergangsfristen. Sie betreffend im Wesentlichen folgende Bereiche: Einwilligungserfordernis für die Weitergabe von Personendaten; Stärkung der Rechtsstellung der Aufsichtsbehörden; klare Anforderungen an die vertragliche Regelung der Auftragsdatenverarbeitung; neue Bestimmungen zum Arbeitnehmerdatenschutz; Werbung und Adresshandel.

Datenschutzrechte von Israel und Andorra

Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahmen vom 1. Dezember 2009 (WP 165 und WP 166) die Datenschutzgesetzgebungen von Israel und Andorra beurteilt. Sie kommt zum Schluss, dass die beiden Länder grundsätzlich ein angemessenes Schutzniveau im Sinne von Art. 25 Abs. 6 DSRL gewährleisten.

Abkürzungen

BCRs:	Binding Corporate Rules
BDSG	Deutsches Bundesdatenschutzgesetz
DSG:	Schweizerisches Bundesgesetz über den Datenschutz vom 1992
DSRL:	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates von 1995
EDÖB:	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU:	Europäische Union
EWR:	Europäischer Wirtschaftsraum
VDSG:	Schweizerische Verordnung zum Bundesgesetz über den Datenschutz von 1993
VDSZ	Schweizerische Verordnung über die Datenschutzzertifizierung von 2007

Der Inhalt dieses Bulletins stellt keine Rechtsauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an:

RUOSS VÖGELE PARTNER | TELEFON +41 44 250 43 00 | www.rvpartner.ch

Auf www.rvpartner.ch verfügbare Bulletins und Broschüren in PDF-Form

2010

- Entwicklungen im schweizerischen Banken- und Kapitalmarktrecht 2010/1 / Swiss Banking and Capital Market Law Update 2010/1
  (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Versicherungsrecht 2010/1 / Swiss Insurance Law Update 2010/1
  (Dr. Alois Rimle, LL.M.)
- Rechtliche Rahmenbedingungen der Unternehmenssanierung

2009

- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/2 / Swiss Insurance, Banking and Capital Market Law Update 2009/2
  (Dr. Alois Rimle, LL.M.)
- Unternehmensleitung in Krisenzeiten Worauf es zu achten gilt
  (Dr. Franziska Buob)
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/1 / Swiss Insurance, Banking and Capital Market Law Update 2009/1
  (Dr. Alois Rimle, LL.M.)
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/1 / Update on Data Protection Law for Companies in Switzerland and the EU 2009/1
  (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Transaktionsrecht 2009/1
  (RVP)

2008

- Revision des Revisionsrechtes: Eine Übersicht über die wichtigsten Neuerungen
  (Sara Sager)
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2008/2 / Swiss Insurance, Banking and Capital Market Law Update 2008/2
  (Dr. Alois Rimle, LL.M.)
- Vom Prozessieren
  (Dr. Franziska Buob)
- Liegenschaften im Erbgang: Häufige Tücken und Fallen (Teil I: Nachlassplanung)
  (Pio R. Ruoss)
- Outsourcing
  (Dr. Marc M. Strolz)
- IP IT Outsourcing
  (Pascale Gola, LL.M.)
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht
- 2008/1 / Swiss Insurance, Banking and Capital Market Law Update 2008/1
  (Dr. Alois Rimle, LL.M.)

2007

- Aktuelles aus dem Bereich des Immaterialgüter- und Firmenrechts
  (Dr. Martina Altenpohl)
- Die „kleine Aktienrechtsreform“ und Neuerungen im Recht der GmbH
  (Chasper Kamer, LL.M.)
- Swiss Insurance Law Update 2007/1
  (Dr. Alois Rimle, LL.M.)
- Privatbestechung (Art. 4a UWG)
  (Dr. Reto T. Ruoss)
- Neue Phase der Freizügigkeit für EU/EFTA-Bürger, deren Familienangehörige und Erbringer von Dienstleistungen in der Schweiz
  (Alfred Gilgen, LL.M.)
- Revidiertes Datenschutzrecht für Unternehmen in der Schweiz
  (Dr. Alois Rimle, LL.M.)
- Aktuelles aus dem Bereich des Wettbewerbs- und Immaterialgüterrechts
  (Chasper Kamer, LL.M.)
- Actions Required under New Swiss Collective Investment Schemes Act
  (Dr. Alois Rimle, LL.M.)

2006

- Dokumenten- und Datenaufbewahrung im schweizerischen Unternehmen
  (Dr. Alois Rimle, LL.M.)
- Schweizerische Versicherungs- und Vermittleraufsicht
  (Dr. Alois Rimle, LL.M.)