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 im Jahr 2011

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

Zürich, Februar 2012, Nr. 1

Inhalt

Unternehmens-Datenschutzrecht der Schweiz

Einsichtsrecht des Bankkunden (Entscheid)

Das Recht auf Einsicht in die eigenen Bankunterlagen unter dem Titel des Datenschutzrechts ist seit Jahren umstritten. Namentlich im Zusammenhang mit dem Zusammenbruch von Lehman Brothers verlangten viele Anleger Einsicht. Die Praxis der Banken war im Bereich des Einsichtsrechts bisher ganz unterschiedlich: Während die einen Banken grosszügig Auskunft erteilten, verweigerten andere Banken jegliche Herausgabe. Mit dieser Thematik befasste sich 2010 das Bezirksgericht Zürich und 2011 das Obergericht Zürich.

Zwischen der Credit Suisse („CS“) und zwei Anlegern bestand ein Streit darüber, ob die Bank hoch spekulative Geschäfte, bei denen die Anleger viel Geld verloren, eigenmächtig getätigt hatte oder aber im Auftrag der beiden Kunden. Aufschluss über die Vorkommnisse hätten die Bankunterlagen geben können, welche die CS aber nicht herausgeben wollte. Daraufhin klagten die beiden Bankkunden gestützt auf das Datenschutzgesetz auf Herausgabe der Unterlagen. Die

Klage wurde vom Bezirksgericht im April 2010 abgewiesen, die Berufung hingegen vom Obergericht im Oktober 2011 gutgeheissen (Beschluss des Obergerichts des Kantons Zürich, I. Zivilkammer, vom 1. Oktober 2011). Darin wird die CS verpflichtet, den Bankkunden Auskunft über sämtliche bankinterne Personendaten zu erteilen, insbesondere betreffend Konto- und Depotbeziehungen, mit Ausnahme sämtlicher interner Notizen zum persönlichen Gebrauch des oder der relevanten Kundenberater.

Gemäss Art. 8 Abs. 1 DSG kann jede Person vom Inhaber einer Datensammlung bzw. Datenverantwortlichen Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Der Datenverantwortliche muss der betroffenen Person daraufhin alle über sie in der Datensammlung vorhandenen Daten mitteilen (Art. 8 Abs. 2 DSG). Gemäss Art. 9 Abs. 4 DSG kann der private Datenverantwortliche die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen es erfordern und er die Personendaten nicht Dritten bekannt gibt.

Die Bank machte vor dem Obergericht geltend, es sei davon auszugehen, dass es beim Auskunftsbegehren um rein finanzielle bzw. zivilprozessuale Beweisinteressen der Bankkunden im Rahmen eines Auftragsverhältnisses gehe. Damit widerspreche das Begehren dem Zweck von Art. 8 DSG. Eine Auskunftsverpflichtung würde die Bank in ihren durch das Zivil- und Zivilprozessrecht verbrieften Verteidigungsrechten beschneiden und mithin ihre überwiegenden Interessen im Sinne von Art. 9 Abs. 4 DSG verletzen. Damit würden die gestellten Auskunftsbegehren nicht wie vom Zweck des Datenschutzgesetzes vorgesehen der Wahrung der Persönlichkeitsrechte, sondern der Verfolgung finanzieller Interessen dienen. Die Bank habe ein legitimes Interesse an der Auskunftsverweigerung, da durch solche offensichtlich zur Prozessvorbereitung gestellte Auskunftsbegehren die materiell-rechtlichen Beschränkungen der Herausgabepflicht und die zivilprozessualen Besonderheiten des Editionsrechts untergraben würden.

Die Bankkunden bestritten vor dem Obergericht, dass sie mit ihren Auskunftsbegehren finanzielle oder zivilprozessuale Beweisinteressen verfolgten. Die internen Aufzeichnungen der Bank seien unrichtig, weil die Instruktionen betreffend hoch spekulative Optionsgeschäfte nie erfolgt seien. Die unrichtige Datenbearbeitung stelle eine Persönlichkeitsverletzung dar, welche das Datenschutzgesetz gerade verhindern wolle. Sie hätten ein datenschutzrechtlich motiviertes Interesse daran, diese Daten berichtigen zu lassen.

Das Obergericht stellt in seinem Entscheid zunächst fest, dass die Bank keine schützenswerte Interessen geltend gemacht habe, welche einer Auskunftserteilung entgegenstehen würden. Die Auskunftsverweigerung ist nicht zur Abwehr unbegründeter Zivilansprüche geeignet. Ob Zivilansprüche aufgrund von Optionsgeschäften bestehen, hängt nicht von einer allfälligen Auskunftserteilung ab. Auch hat die Bank gemäss Obergericht nicht aufgezeigt, inwiefern ihre Interessen durch das zivilprozessuale Editionsrecht besser gewahrt sein sollen.

Nach den Ausführungen des Obergerichts liegt im vorliegenden Fall auch kein Rechtsmissbrauch vor. Da das Auskunftsrecht grundsätzlich auch ohne Interessennachweis ausgeübt werden kann, braucht es auch nicht datenschutzrechtlich motiviert zu sein. Datenschutzgründe können regelmässig vorgeschoben werden. Grundsätzlich kommen auch finanzielle Interessen in Frage, zumal solche Interessen auch zur Verweigerung der Auskunft vorgetragen werden können. Je gewichtigere Interessen der Auskunftsverpflichtete an einer Auskunftsverweigerung hat, desto höhere Anforderungen sind gemäss Obergericht an die Motivierung des Auskunftsrechts zu stellen. Bei der Prüfung, ob das Auskunftsrecht rechtsmissbräuchlich geltend gemacht wurde, ist zu berücksichtigen, dass der Auskunftsverpflichtete zur Verweigerung der Auskunft berechtigt ist, wenn er dafür überwiegende Interessen ins Feld führen kann. Das Rechtsmissbrauchsverbot dient nicht dazu, die Interessenlage zugunsten des Auskunftsverpflichteten zu verschieben, sondern dazu, krasses Unrecht zu verhindern. Selbst wenn die Bankkunden die Auskunft im Hinblick auf einen allfälligen nachfolgenden Schadenersatzprozess verlangt haben sollten, ist dies gemäss Obergericht nicht per se rechtsmissbräuchlich. Wenn die Bank nicht darlegt, inwiefern ihre Interessen durch das zivilprozessuale Editionsrecht besser gewahrt sind, kann dies nicht mit der Berufung auf Rechtsmissbrauch korrigiert werden.

Datenschutz und Urheberrechtsverletzung (Entscheid)

Im Auftrag von Urheberrechtsinhabern sammelte Logistep AG in Peer-to-Peer-Netzwerken IP-Adressen von Nutzern, die angeblich illegal urheberrechtsgeschützte Inhalte (Musik- oder Videodateien) zum Tausch anboten. Mit diesen IP-Adressen stiessen die Rechtsinhaber dann Strafverfahren an, um mittels strafrechtlicher Akteneinsicht die Identität der Betroffenen zu erfahren und von diesen Schadenersatz zu verlangen.

Nach Auffassung des EDÖB war diese Datenbearbeitung für die Betroffenen nicht erkennbar und verletzte das Zweckbindungsprinzip, ohne dass dafür ein Rechtfertigungsgrund vorlag. Als Logistep die Nachforschungen in P2P-Netzwerken entgegen der Empfehlung des EDÖB nicht einstellte, klagte dieser vor Bundesverwaltungsgericht, welches die Klage abwies. Auf Beschwerde des EDÖB hob das Bundesgericht das Urteil des Bundesverwaltungsgerichts auf. Das Bundesgericht wies Logistep an, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und untersagte dem Unternehmen, die bereits beschafften Daten den betroffenen Urheberrechtsinhabern weiterzuleiten (BGE 136 II 508).

Gemäss Art. 12 DSG gilt, dass wer Personendaten bearbeitet, dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen darf. Er darf insbesondere nicht Personendaten entgegen den Grundsätzen der Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG bearbeiten. Art. 4 DSG umfasst u.a. die Grundsätze der Zweckbindung und der Erkennbarkeit. Obwohl in Art. 12 DSG hinsichtlich einer Bearbeitung entgegen den Grundsätzen nicht ausdrücklich auf die Rechtfertigung verwiesen wird, ist die Bestimmung gemäss Bundesgericht so auszulegen, dass eine Rechtfertigung der grundsatzwidrigen Bearbeitung von Personendaten zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden können.

Im vorliegenden Fall stellt gemäss Bundesgericht das Vorgehen von Logistep eine Persönlichkeitsverletzung dar, indem dadurch die Grundsätze der Zweckbindung und der Erkennbarkeit verletzt wurden. Im Weiteren ist die Rechtfertigung durch ein überwiegendes privates oder öffentliches Interesse zu verneinen: Logistep verfolgt ein wirtschaftliches Interesse; das Unternehmen strebt eine Vergütung für seine Tätigkeit an. Die Tätigkeit besteht darin, mit Hilfe einer eigens dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken zu suchen und von deren Anbietern Daten zu speichern. Eine solche Methode führt allgemein wegen fehlender gesetzlicher Reglementierung zu einer Unsicherheit etwa in Bezug auf die Art und den Umfang der gesammelten Daten und deren Bearbeitung. An dieser Einschätzung ändert gemäss Bundesgericht auch das Interesse der Auftraggeber von Logistep, Urheberrechte zu verwerten, nichts. Die Interessen an der wirksamen Bekämpfung von Urheberrechtsverletzungen vermag die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Das überwiegende private oder öffentliche Interesse ist gemäss Bundesgericht umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf.

Das Bundesgericht präzisiert in seinem Entscheid abschliessend, dass vorliegend ein konkreter Fall beurteilt worden sei und es nicht darum gehe, dem Datenschutz generell den Vorrang gegenüber dem Schutz des Urheberrechts einzuräumen. Es sei Sache des Gesetzgebers und nicht des Richters, notwendige Massnahmen zu treffen, um einen den neuen Technologien entsprechenden Urheberrechtsschutz zu gewährleisten.

Cloud Computing

Der EDÖB befasste sich 2011 im Rahmen besonderer Erläuterungen mit „Cloud Computing“: Danach lagern immer mehr Unternehmen ihre bisher typischerweise intern erledigten Datenverarbeitungen aus Kostengründen an externe Unternehmen aus. Sie setzen auf „Cloud Computing“. Dieser Begriff aus dem IT bedeutet, dass Software, Speicherkapazitäten oder Rechnerleistung über ein Netzwerk, z.B. das Internet oder innerhalb eines Virtual Private Network (VPN) bedarfsorientiert bezogen, d.h. gemietet werden. Die IT-Landschaft (z.B. Rechenzentrum, Datenspeicher, Mail- oder Kollaborationssoftware, Entwicklungsumgebungen oder Spezialsoftware wie CRM) steht nicht mehr im Eigentum des Unternehmens und wird nicht mehr von diesem selbst betrieben, sondern von einem oder mehreren Cloud-Service-Anbietern als

Dienstleistung gemietet. Die Anwendungen befinden sich nicht mehr im eigenen Netz, sondern im Cloud. Der Zugang zu Daten, Services und Infrastruktur, die im Cloud verfügbar sind, erfolgt mittels Fernzugriff (remote access).

Datenschutzrechtlich handelt es sich um eine Datenbearbeitung durch Dritte im Sinne von Art. 10a DSG (Outsourcing), wenn bei der Nutzung von Cloud Computing Personendaten bearbeitet werden. Es müssen dabei Vorschriften über Auswahl, Instruktion und Überwachung, Unterauftragsbearbeitung, Datensicherheit, Datenbekanntgabe ins Ausland sowie Auskunfts-, Löschungs- und Berichtigungsrechte beachtet werden. Der Cloud-Nutzer bleibt als Datenverantwortlicher und Auftraggeber letztlich gegenüber den betroffenen Personen für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und haftet bei deren Verletzungen diesen gegenüber.

Ausländische Unterauftragnehmer

Gemäss Art. 10a DSG dürfen die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte. Aus dieser Verpflichtung kann abgeleitet werden, dass ein Auftragnehmer, falls er für die Datenbearbeitung einen Unterauftragnehmer beiziehen will, mit diesem eine Vereinbarung abschliessen muss, und dass auch der Unterauftragnehmer die Daten nur so bearbeiten darf, wie es der Auftraggeber selbst tun dürfte. Diese Regelung gilt für die Auftragsbearbeitung (Outsourcing) sowohl im In- als auch im Ausland. Bei einer Auftragsbearbeitung im Ausland gelten zudem die Anforderungen von Art. 6 DSG.

Dementsprechend sieht der überarbeitete Mustervertrag des EDÖB für das Outsourcing von Datenbearbeitungen ins Ausland vor, dass eine Datenbearbeitung durch einen Unterauftragnehmer nur mit vorgängiger schriftlicher Zustimmung des Auftraggebers zulässig ist. Zudem wird der Auftragnehmer verpflichtet, mit dem Unterauftragnehmer einen schriftlichen Vertrag abzuschliessen. Darin verpflichtet sich dieser, dieselben Datenschutzstandards einzuhalten, wie sein (direkter) Auftraggeber. Diese Regelung entspricht im Wesentlichen den geänderten EU-Standardvertragsklauseln für Controller-to-Processor-Transfers (siehe hinten).

Safe Harbor und Unterauftragsbearbeitung

Datenbekanntgaben an US-Unternehmen, die nach dem U.S.-Swiss Safe Harbor Framework zertifiziert sind, fallen nach Ansicht des EDÖB nicht unter Art. 6 Abs. 2 DSG (grenzüberschreitende Bekanntgabe in ein Land ohne angemessenen Datenschutz). Durch die Registrierung unter dem Safe Harbor Framework erreicht das US-Unternehmen ein Datenschutzniveau, das von der Schweiz als angemessen anerkannt wird. Hingegen bleibt Art. 10a DSG (Datenbearbeitung durch Dritte) anwendbar, wenn ein Schweizer Unternehmen Daten an einen Safe-Harbor-zertifizierten Empfänger im Rahmen einer Auftragsbearbeitung bekannt gibt. Danach dürfen die Daten im Rahmen einer Auftragsbearbeitung nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte. Der Auftraggeber muss sich vergewissern, dass der Auftragsbearbeiter die Datensicherheit gewährleistet.

Im Fall einer Unterauftragsbearbeitung muss der Auftragsbearbeiter gemäss Art. 10a DSG für die Datenbearbeitung durch den Subunternehmer einstehen und sich vergewissern, dass die Datensicherheit gewährleistet ist. Dementsprechend muss sich der schweizerische Datenverantwortliche die Kontrolle und das Weisungsrecht in Bezug auf die Datenbearbeitung durch den Safe-Harbor-zertifizierten Auftragsbearbeiter und dessen allfällige Subunternehmer wirksam sichern. Es folgt, dass der schweizerische Datenverantwortliche mit dem Auftragsbearbeiter einen schriftlichen Vertrag abschliessen muss, der verschiedene Bestimmungen enthält, wie sie auch in den EU-Mustervertragsklauseln und dem Mustervertrag des EDÖB enthalten sind.

Diese Anforderung nach schweizerischem Datenschutzrecht gilt unabhängig davon, dass das Safe Harbor Framework selbst den Weitertransfer an einen Unterauftragsbearbeiter nach dem Onward-Transfer-Prinzip erlaubt, ohne dass der schweizerische Datenexporteur seine Zustimmung erteilt hat oder überhaupt davon weiss und ohne dass ein in der Schweiz üblicher Datentransfervertrag abgeschlossen wird. Somit können sich US-Unternehmen nicht auf den Standpunkt stellen (was sie in der Praxis oftmals tun), dass mit der Zertifizierung unter dem U.S.-Swiss Safe Harbor Framework und der damit verbundenen Verpflichtung zur Einhaltung der Safe Harbor-Grundsätze

dem Datenschutz ausreichend entsprochen werde. Es sind auf der Grundlage des schweizerischen Datenschutzrechts vielmehr Verpflichtungen zu beachten, die über das Safe Harbor Framework hinausgehen (z.B. Genehmigung von Subunternehmern, Überbindung von Datenschutzpflichten auf Subunternehmer).

Outsourcing und Patientengeheimnis

Gemäss Art. 10a DSG ist eine Auftragsbearbeitung (Outsourcing) u.a. nur zulässig, wenn keine gesetzliche Geheimhaltungspflicht es verbietet. Im medizinischen Bereich stellt sich die Frage, ob das Patientengeheimnis eine Auftragsbearbeitung zulässt.

Das Patientengeheimnis, dessen Verletzung strafrechtlich sanktioniert ist (Art. 321 StGB), stellt eine gesetzliche Geheimhaltungspflicht dar. Trotzdem ist die Auftragsbearbeitung bei Ärzten und Kliniken eine alltägliche Praxis, in der Regel ohne dass dabei die Einwilligung der Patienten eingeholt wird. Das Bundesamt für Justiz versucht den gegenwärtigen Zustand damit zu rechtfertigen, dass die von Ärzten oder Kliniken beauftragten Datenbearbeiter als Hilfspersonen zu betrachten seien und deshalb keine Auftragsbearbeitung im Sinne des Datenschutzgesetzes vorliege. Dieser Auffassung kann nicht zugestimmt werden. Es liegt m.E. in solchen Fällen regelmässig eine Auftragsbearbeitung vor. Für Ärzte und Kliniken ist es deshalb empfehlenswert, die Einwilligung der Patienten für die Datenbearbeitung durch Dritte einzuholen, allenfalls im Rahmen einer Bestimmung im Aufnahmeformular (vgl. auch 18. Tätigkeitsbericht 2010/2011 des EDÖB, S. 65).

Marketing durch Krankenversicherer

In der Vergangenheit haben verschiedene Krankenversicherer Personendaten von versicherten Personen mit einer bestimmten Medikation verwendet, um sie schriftlich auf günstigere Medikamente hinzuweisen, die für sie ebenfalls geeignet sein könnten.

Der EDÖB hat entsprechende Sachverhaltsabklärungen vorgenommen und ist zum Schluss gekommen, dass diese Vorgehensweise eine Datenschutzverletzung darstellt: Krankenkassen, die im Bereich der obligatorischen Krankenversicherung tätig sind, gelten als Bundesbehörden, weil sie eine öffentliche Aufgabe des Bundes vollziehen. Es gilt für sie somit das Legalitätsprinzip. Gemäss Art. 17 DSG dürfen Organe des Bundes Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen bedarf es grundsätzlich eines Gesetzes im formellen Sinn. Das Bundesgesetz über die Krankenversicherung hält fest, für welche Zwecke die Krankenversicherer Daten von versicherten Personen (auch besonders schützenswerte) bearbeiten dürfen. Das direkte Anpreisen von Medikamenten gehört nicht dazu (18. Tätigkeitsbereich 2010/2011 des EDÖB, S. 74).

Adresshandel und Auskunfteien in Abklärung

Der EDÖB stellt in seinem Tätigkeitsbericht 2010/2011 fest, dass die Datenbearbeitung im Adresshandel sowie die Bearbeitung von Bonitäts- und Wirtschaftsdaten durch Auskunfteien den Regeln des Datenschutzgesetzes unterstehen. Gemäss Tätigkeitsbericht werden zurzeit weitere Abklärungen vorgenommen, um festzustellen, ob in der gegenwärtigen Praxis den datenschutzrechtlichen Anforderungen entsprochen wird (18. Tätigkeitsbericht 2010/2011 des EDÖB, S. 85 und 89).

Analysesoftware für Internetseiten

Tools wie Google Analytics, Piwik, Google Urchin oder Clicky liefern Websiteanbietern Informationen zum Nutzungsverhalten der Besucher. Sie analysieren u.a. die Anzahl Klicks, die besuchten Seiten, die Verweildauer, den Standort des Users oder die Internetseiten, die er zuvor besucht hat. Einige Tools übertragen diese Informationen zusammen mit der IP-Adresse an den Firmenserver des Programmanbieters. Dieser kommt so in den Besitz von Daten, die möglicherweise Rückschlüsse auf Vorlieben oder Einstellungen der einzelnen Nutzer erlauben.

Der EDÖB wies 2011 darauf hin, dass Webseiten unabhängig vom eingesetzten Programm in der Datenschutzerklärung umfassend über die im Rahmen der Auswertung erhobenen Daten und deren Verwendung informieren müssen (datum 01/2011).

Vorläufiger Verzicht auf Zertifizierung von Produkten und Dienstleistungen

Der EDÖB weist in seinem Tätigkeitsbericht von 2010/2011 auf verschiedene technische und rechtliche Probleme im Bereich der Zertifizierung von Produkten und Dienstleistungen hin. Er hat angesichts dieser Probleme und unter Berücksichtigung der Tatsache, dass auch etwa Deutschland und Frankreich bei der Einführung einer Zertifizierung von Produkten und/oder Dienstleistungen Schwierigkeiten haben, beschlossen, die Arbeiten in diesem Bereich vorläufig einzustellen (18. Tätigkeitsbericht 2010/2011 des EDÖB, S. 19). Die Thematik wird möglicherweise im Rahmen einer Revision des Datenschutzgesetzes wieder aufgenommen (siehe unten).

Observation durch Privatdetektiv (Entscheid)

Ein Haftpflichtversicherer hatte einen Privatdetektiv mit der Überwachung eines anspruchsstellenden Geschädigten beauftragt, worauf dieser auf Unterlassung, Herausgabe aller Unterlagen sowie Zahlung einer Genugtuung klagte. Das Bundesgericht musste u.a. die Frage prüfen, ob mit der Observation die Persönlichkeitsrechte (Art. 28 ZGB) des Observierten widerrechtlich verletzt worden waren.

Es stellte sich dem Bundesgericht zunächst die Frage, ob das Recht auf Schutz der Geheim- und Privatsphäre oder das Recht am eigenen Bild verletzt worden war. Lag eine Persönlichkeitsverletzung vor, so stellte sich dem Bundesgericht weiter die Frage nach einer möglichen Rechtfertigung. Rechtfertigungsgründe sind die Einwilligung des Verletzten sowie überwiegende öffentliche oder private Interessen.

Vorliegend bejahte das Bundesgericht eine Verletzung der Persönlichkeitsrechte, erachtete diese aber durch die überwiegenden Interessen des Versicherers und der dahinter stehenden Versicherungsgemeinschaft, keine Leistungen zu Unrecht erbringen zu müssen, als gerechtfertigt. Das Interesse des Versicherers an einer wirksamen Missbrauchsbekämpfung wurde höher eingeschätzt als das Interesse des Observierten auf Unversehrtheit seiner Persönlichkeit (BGE 136 III 410).

Anpassung des DSG an den Rahmenbeschluss 2008/977

Mit dem Inkrafttreten des Bundesgesetzes über die Umsetzung des Rahmenbeschlusses 2008/977 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen am 1. Dezember 2010 wurde auch das schweizerische Datenschutzgesetz geändert.

In Bezug auf die Datenbearbeitung durch Private ergaben sich im Wesentlichen folgende Anpassungen: Der frühere Art. 7a (Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen) wurde als neuer Art. 14 in den 3. Abschnitt des Datenschutzgesetzes verschoben, der das Bearbeiten von Personendaten durch Private regelt. Zudem wurde Art. 9 DSG redaktionell an die Aufhebung von Art. 7a angepasst; Art. 9 DSG regelt nunmehr nur noch Einschränkungen des Auskunftsrechts. Schliesslich verbessern verschiedene neue Bestimmungen (Art. 26, 26a, 26b und 30 DSG) die institutionellen Garantien der Unabhängigkeit des EDÖB. Insbesondere ist neu die Wahl des Beauftragten durch den Bundesrat einer Genehmigung durch die Bundesversammlung unterworfen, wobei die Wiederwahl hingegen keiner solchen Genehmigung bedarf.

Überprüfung des geltenden Datenschutzrechts

Der Bundesrat hat am 9. Dezember 2011 einen Bericht über die geplante Anpassung des Datenschutzrechts in der Schweiz veröffentlicht. Der Bundesrat ortet verschiedene Problembereiche, die er mit der geplanten Revision angehen will: Zunächst geht es um höhere Anforderungen an neue Technologien. Allfällige datenschutzrechtliche Probleme sollen bereits bei der Entwicklung neuer Technologien geprüft (ev. Zertifizierung) und nicht erst nachträglich behoben werden. Im Weiteren soll das „Recht auf Vergessen“ im Internet präzisiert werden, eventuell durch das automatische Löschen von Daten nach einer gewissen Zeit. Die Nutzer sollen die Herrschaft über einmal bekannt gegebene Daten behalten können. Schliesslich sollen auch die Ausweitung der Informationspflicht bei der privaten Datenbeschaffung und die Einführung einer Verbandsklage geprüft werden (siehe NZZ vom 10. Dezember 2011, S. 13).

Unternehmens-Datenschutzrecht der EU

Neues EU-Datenschutzrecht im Entwurf

Die Europäische Kommission hat am 25. Januar 2012 eine umfassende Reform der aus dem Jahr 1995 stammenden EU-Datenschutzvorschriften vorgeschlagen. Die technischen Fortschritte und die Globalisierung haben die Art, wie Daten erhoben, abgerufen und verwendet werden, grundlegend verändert. Die datenschutzrechtlichen Grundsätze sollen deshalb aktualisiert und modernisiert werden, damit der Schutz personenbezogener Daten auch in Zukunft garantiert ist.

Die EU-Datenschutzrichtlinie von 1995 soll durch eine *Verordnung* ersetzt werden, die in allen Mitgliedsländern direkt anwendbar sein wird. Damit bedarf es keiner nationalen Umsetzungsgesetzgebung mehr. Bis zur Inkraftsetzung der Verordnung wird zwar noch einige Zeit vergehen (zwei Jahre nach Annahme), doch ist zu erwarten, dass Unternehmen schon vorher beginnen werden, die neuen Anforderungen zu implementieren. Die wichtigsten geplanten Änderungen werden nachfolgend kurz dargestellt:

Der geographische Geltungsbereich des EU-Rechts soll ausgedehnt werden. Die ausserhalb der EU erfolgende Datenverarbeitung durch auf dem EU-Markt aktive Unternehmen, die ihre Dienste den EU-Bürgern anbieten, soll künftig den EU-Vorschriften unterliegen. Viele solche Unternehmen werden in der EU einen Vertreter bezeichnen müssen.

Die Sanktionen bei datenschutzrechtlichen Verstössen sollen verschärft werden. Die Aufsichtsbehörden können nach dem Verordnungsentwurf Geldbussen gegen Unternehmen bis zu 2% des weltweiten Jahresumsatzes aussprechen. Vor dem Hintergrund solch massiver Sanktionen und verschärfter Kontrollen dürfte es für Unternehmen mit Geschäftstätigkeit im EU-Raum keine Option mehr sein, datenschutzrechtliche Verantwortlichkeiten zu vernachlässigen.

Datenverantwortliche Unternehmen haben nach dem Verordnungsentwurf mehr Verantwortung und verstärkte Rechenschaftspflichten. Zwar sollen verschiedene Meldepflichten für Unternehmen beseitigt werden. Doch müssen Unternehmen neu Verarbeitungsoperationen dokumentieren und die Dokumentation aufbewahren und für allfällige Anfragen der Aufsichtsbehörde bereithalten. Sie müssen bei riskanten Bearbeitungsarten eine Datenschutz-Folgeabschätzung durchführen. Sie müssen organisatorische Massnahmen und Verfahren durchsetzen, die sicherstellen, dass die Verarbeitung datenschutzkonform erfolgt („data protection by design", „data protection by default"). Sie müssen die Aufsichtsbehörde über Datenschutzverstösse ohne unangemessene Verzögerung und nach Möglichkeit innerhalb von 24 Stunden informieren. Schliesslich müssen Unternehmen, die mehr als 250 Mitarbeitende beschäftigen, einen unabhängigen Datenschutzbeauftragten ernennen.

Auch für auftragsverarbeitende Unternehmen ergeben sich aus dem Verordnungsentwurf direkte Pflichten. Sie müssen die Sicherheit der Verarbeitung sicherstellen und entsprechende Massnahmen umsetzen. Sie müssen die erforderliche Dokumentation über die Datenverarbeitung erstellen. Sie müssen den Datenverantwortlichen bei der Durchführung der Datenschutz-Folgeabschätzung unterstützen. Sie müssen schliesslich den Datenverantwortlichen über allfällige Datenschutzverstösse umgehend informieren.

Das Regelungskonzept für den grenzüberschreitenden Datentransfer wird im Verordnungsentwurf grundsätzlich beibehalten. Es wird allerdings ein neuer Ausnahmetatbestand eingeführt, bei dem ein Datentransfer in ein Land ohne angemessenen Datenschutz auch ohne Garantien zulässig ist: Danach soll ein solcher Datentransfer grundsätzlich zulässig sein, wenn er zur Verwirklichung des berechtigten Interesses des Datenverantwortlichen erforderlich ist und nicht als häufig oder massiv bezeichnet werden kann. Im Weiteren anerkennt der Verordnungsentwurf ausdrücklich die „Binding Corporate Rules" nicht nur für Datenverantwortliche, sondern auch für Auftragsverarbeiter. Allerdings dürfte dieser Ansatz für global tätige Unternehmen eher weniger attraktiv sein, u.a. deshalb, weil sämtliche Mitglieder der Unternehmensgruppe erfasst sein müssen.

Die Rechte der betroffenen Personen werden im Verordnungsentwurf allgemein gestärkt. Die Einwilligung der betroffenen Person liegt nur bei einer *expliziten* Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung vor, wobei die Beweislast beim Datenverantwortlichen liegt. Wenn ein

klares Ungleichgewicht zwischen Datenverantwortlichem und betroffener Person besteht wie etwa im *Fall des Arbeitsverhältnisses*, vermag die Einwilligung keinen Rechtfertigungsgrund für die Datenbearbeitung zu liefern. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so muss die betroffene Person das Recht haben, Widerspruch einzulegen. Die betroffenen Personen sollen bei Onlinediensten das Recht haben, ihre eigenen Daten zu löschen, wenn keine legitimen Gründe für deren Aufbewahrung bestehen, und sollen die Unterlassung jeglicher weiterer Verarbeitung dieser Daten verlangen können („Recht auf Vergessen"). Hat der Datenverantwortliche die Daten öffentlich gemacht, so muss er alle vertretbaren Schritte (auch technischer Art) unternehmen, um verarbeitende Dritte darüber zu informieren, dass die betroffene Person von ihnen die Löschung aller Querverweise oder von Kopien oder Replikationen verlangt. Schliesslich wird das Recht der betroffenen Person auf Datenportabilität eingeführt. Dabei geht es um das Recht der betroffenen Person, ihre Daten aus einem automatischen Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der Datenverantwortliche sie daran hindern kann. Als Folge davon wird der Wettbewerb unter den Anbietern derartiger Dienste zunehmen.

Es soll in der EU das System des „lead regulator" oder „one stop shop" eingeführt werden: Bei Niederlassungen in mehreren EU-Mitgliedstaaten soll die Aufsichtsbehörde des Mitgliedstaates für die Aufsicht zuständig sein, in dem sich die Hauptniederlassung des Datenverantwortlichen oder Auftragsverarbeiters befindet.

Es ist im Verordnungsentwurf schliesslich vorgesehen, dass ein Europäischer Datenschutzausschuss eingesetzt wird. Dieser setzt sich aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedsstaates und dem Europäischen Datenschutzbeauftragten zusammen. Dieser Ausschuss wird die Artikel-29-Datenschutzgruppe ersetzen. Seine Aufgabe wird es etwa sein, Stellungnahmen im Interesse der einheitlichen Rechtsanwendung abzugeben und die EU-Kommission in datenschutzrechtlichen Fragen zu beraten.

Neue ePrivacy Richtlinie

Die e-Privacy-Richtlinie der EU (Richtlinie 2009/136/EG) wurde erlassen, um den Anforderungen der neuen digitalen Technologien gerecht zu werden. Die Richtlinie ergänzt die EU-Datenschutzrichtlinie von 1995 und umfasst alle Themen im Bereich der Privatsphäre im Sektor der elektronischen Kommunikation. Die Richtlinie behandelt den Schutz der Personendaten sowie der Privatsphäre in elektronischen Kommunikationssystemen. Sie sieht vor, dass die EU-Mitgliedsstaaten die Normen bis zum 25. Mai 2011 in nationales Recht umgesetzt haben müssen.

Die neue Richtlinie verpflichtet die Dienstanbieter erstmals zur aktiven Information ihrer Nutzer über Datenpannen sowie spezifische Risiken wie Viren oder Malware-Attacken.

Eine weitere Neuerung besteht darin, dass die Nutzer ausdrücklich in die Platzierung von *Cookies* oder Spyware einwilligen müssen (Opt-in-Verfahren). Ohne Zustimmung des Internetnutzers darf solche Software nicht mehr auf dessen PC installiert werden. Dazu müssen sie vorgängig klar und umfassend über die Zwecke der Speicherung oder des Zugangs informiert werden. Von der Einwilligungspflicht ausgenommen sollen Verfahren sein, deren „alleiniger Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist", damit ein ausdrücklich gewünschter Dienst zur Verfügung gestellt werden kann (so genannte „Session-Cookies" z.B. bei der Authentifizierung für einen bestimmten Dienst).

Konzept der datenschutzrechtlichen Einwilligung

Die Artikel-29-Datenschutzgruppe publizierte 2011 eine Stellungnahme zum Begriff der Einwilligung (Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP 187). Sie nimmt eine gründliche Analyse des Konzepts der Einwilligung vor, wie es gegenwärtig in der EU-Datenschutzrichtlinie und der e-Privacy Richtlinie der EU zur Anwendung kommt.

Die Datenschutzgruppe stellt in ihrer Stellungnahme u.a. fest, dass die Einwilligung einen von mehreren Rechtfertigungsgründen für die Bearbeitung von Personendaten darstellt. Die Einwilligung hat nach Auffassung der Datenschutzgruppe eine grosse Bedeutung, schliesst aber die Möglichkeit nicht aus, je nach

Kontext andere Rechtfertigungsgründe zu verwenden, die vielleicht aus Sicht sowohl des Datenverantwortlichen als auch der betroffenen Person angemessener sind. Wenn die Zustimmung korrekt zur Anwendung gebracht wird, ist sie ein Instrument, das der betroffenen Person Kontrolle über die Verarbeitung ihrer Daten gibt. Wenn die Zustimmung hingegen inkorrekt verwendet wird, wird die Kontrolle durch die betroffene Person illusorisch und die Zustimmung stellt eine ungeeignete Grundlage für die Datenbearbeitung dar.

Geldwäschereibekämpfung und Datenschutz

Die Artikel-29-Datenschutzgruppe publizierte 2011 eine Stellungnahme über Datenschutzaspekte im Zusammenhang mit der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung (Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, adopted on 13 June 2011, WP 186). Dabei werden 44 Empfehlungen für den angemessenen Umgang mit datenschutzrechtlichen Fragestellungen im Rahmen der Geldwäschereibekämpfung abgegeben.

Anwendbares EU-Datenschutzrecht

Die Artikel-29-Datenschutzgruppe publizierte Ende 2010 eine Stellungnahme zum anwendbaren Recht (Stellungnahme 8/2010 zum anwendbaren Recht, angenommen am 16. Dezember 2010, WP 179). Darin wird der Anwendungsbereich der EU-Datenschutzrichtlinie präzisiert. Es geht insbesondere um Artikel 4, der bestimmt, welche auf der Grundlage der Datenschutzrichtlinie erlassenen einzelstaatlichen Vorschriften auf die Verarbeitung personenbezogener Daten Anwendung finden. Eine klare Vorstellung davon, welches Recht zur Anwendung kommt, wird den Datenverantwortlichen, betroffenen Personen und anderen Beteiligten mehr Rechtssicherheit vermitteln.

Regelung der Unterauftragsverarbeitung in EU-Standardvertragsklauseln

Der Beschluss 2010/87/EU der Europäischen Kommission über die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der EU-Datenschutzrichtlinie, der 2010 in Kraft getreten ist, enthält neu die Voraussetzungen für die Vergabe eines Unterauftrags. Wenn der Datenexporteur (als Datenverantwortlicher) mit dem Datenimporteur (als Auftragsverarbeiter) den Datenschutzvertrag abschliesst, kann letzterer gemäss Vertragsklauseln für die Ausführung des Verarbeitungsauftrages einen Unterauftragnehmer einsetzen. Die Artikel-29-Datenschutzgruppe hat in einer Publikation von 2010 versucht, verschiedene Aspekte der Unterauftrags-Vergabe zu klären (WP176). Die wichtigsten Ergebnisse dieser Klärung werden nachfolgend kurz zusammengefasst.

Die Standardvertragsklauseln kommen zur Anwendung, wenn der Datenexporteur im EWR niedergelassen ist und ein in einem Drittland niedergelassener Auftragsverarbeiter einen ebenfalls in einem Drittland niedergelassenen Unterauftragsverarbeiter mit seinen Verarbeitungsdiensten beauftragt. Hingegen sind gemäss Datenschutzgruppe die Standardklauseln für die Verwendung für einen Auftragsverarbeiter im EWR unangemessen. Für Fälle, bei denen der Autragsverarbeiter im EWR und der Unterauftragsverarbeiter in einem Drittland niedergelassen sind, bieten sich folgende Alternativen an: (1) Direktverträge zwischen dem Datenverantwortlichen im EWR und Auftragsverarbeitern in Drittländern; (2) Auftrag des Datenverantwortlichen im EWR an den Auftragsverarbeiter im EWR, die Standardvertragsklauseln im Namen des Ersteren zu verwenden; oder (3) Ad-hoc-Verträge.

Gemäss Klausel 11 Ziffer 1 der Standardvertragsklauseln darf der Datenimporteur ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen Verarbeitungsauftrag an einen Unterauftragnehmer vergeben. Dabei wird offengelassen, ob der Datenverantwortliche mit einer vorherigen schriftlichen Zustimmung die Vergabe von Unteraufträgen generell erlauben oder die Vergabe jedes Unterauftrags einzeln genehmigen muss. Nach Auffassung der Datenschutzgruppe muss der Datenverantwortliche entscheiden, ob eine generelle vorherige Zustimmung ausreicht oder ober für jeden Unterauftrag erneut eine Zustimmung erteilt werden muss. Dabei dürften etwa die Rahmenbedingungen der Verarbeitung und die Art der Daten (einfache oder besonders schützenswerte) berücksichtigt werden.

Wenn Auftragsverarbeiter, die nicht im EWR niedergelassen sind, von einem Datenimporteur Daten erhalten (im Rahmen eines mit dem Datenexporteur

geschlossenen Globalvertrages), sind sie entweder Unterauftragsverarbeiter oder weitere Datenimporteure. Dabei ist massgebend, wer den Auftrag erteilt hat. Sind sie vom Datenexporteur beauftragt worden, so handelt es sich um weitere Datenimporteure. Sind sie vom Datenimporteur oder einem Unterauftragnehmer des Datenimporteurs beauftragt worden, so handelt es sich um Unterauftragsverarbeiter.

Wenn ein Datenimporteur Daten an einen Unterauftragsverarbeiter übermittelt, der im Auftrag mehrerer Datenexporteure für den Datenimporteur Leistungen erbringt, ist es gemäss Datenschutzgruppe grundsätzlich nicht möglich, alle Aufträge in einem einzigen Vertrag zusammenzufassen. Anhang 1 des Vertrages (zu den Standardvertragsklauseln) kann regelmässig nicht für alle Aufträge gleich sein, da die Identität des Datenexporteurs und wohl auch die Datenkategorien, die betroffenen Personen und die Beschreibung der Verarbeitungsvorgänge unterschiedlich sein werden.

Schliesslich weist die Datenschutzgruppe darauf hin, dass der Unterauftragsverarbeiter auch einfach den Vertrag (inkl. Standardvertragsklauseln) zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnen kann. Auf diese Weise ist die Anforderung einer schriftlichen Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter, mit der diesem die gleichen Pflichten auferlegt werden, erfüllt.

Abkürzungen

BGE:	Bundesgerichtsentscheid
CRM:	Customer Relationship Management
DSG:	Schweizerisches Bundesgesetz über den Datenschutz von 1992
EDÖB:	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU:	Europäische Union
EWR:	Europäischer Wirtschaftsraum
StGB:	Schweizerisches Strafgesetzbuch von 1937
ZGB:	Schweizerisches Zivilgesetzbuch von 1907

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

2011

- Entwicklungen im schweizerischen Transaktionsrecht 2/2011 (Deutsch und Englisch)
- (Dr. Alois Rimle, LL.M.)
- Geplante Änderungen im schweizerischen Versicherungsvertragsrecht in Kürze (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Eigenkapitalanforderungen und Eigenkapitalschutz im schweizerischen Aktien- und Aufsichsrecht (eine Übersicht) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Versicherungsrecht 2011/1 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Transaktionsrecht 2011/1 (RVP)
- Vermeidung der Regulierung von Private Equity-Investitionen in der Schweiz (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.; Alfred Gilgen, LL.M., N.Y. BAR)
- Durchsetzung von Geldforderungen nach der neuen ZPO (Dr. Alois Rimle, LL.M.)

2010

- Der Aktionärbindungsvertrag (Chasper Kamer, LL.M.)
- Entwicklungen im schweizerischen Transaktionsrecht 2010/1 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU 1/2010 (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Banken- und Kapitalmarktrecht 2010/1 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im schweizerischen Versicherungsrecht 2010/1 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Rechtliche Rahmenbedingungen der Unternehmenssanierung (RVP)

2009

- Entwicklungen im schweizerischen Transaktionsrecht 2009/2 (Deutsch und Englisch) (RVP)
- Überstunden und Überzeit (Dr. Franziska Buob)
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/2 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/2
- Unternehmensleitung in Krisenzeiten Worauf es zu achten gilt (Dr. Franziska Buob)
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/1 (Deutsch und Englisch) (Dr. Alois Rimle, LL.M.)
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/1 (Deutsch und Englisch) (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 (Deutsch und Englisch) (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 (Deutsch und Englisch) (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.)