

Orientierung

Dominika Blonski

Datenschutz – Kundendaten nutzen und schützen

Tagung des Europa Instituts an der Universität Zürich vom 28. Januar 2009

Inhaltsübersicht

- I. Einführung
- II. Erste Erfahrungen mit dem revidierten Datenschutzgesetz
- III. Schnittstellen und Reibungsflächen – Datenschutz im Unternehmensalltag
- IV. Die Bearbeitung von Personendaten zu Marketingzwecken – «the dos and don'ts»
- V. Risikomanagement im Datenschutz – Grundsätzliches und Lessons Learned aus den jüngsten Datenschutzvorfällen
- VI. Internetdienste und Datenschutz

I. Einführung

Anlässlich des 3. Europäischen Datenschutztages organisierte das Europa Institut am 28. Januar 2009 eine Tagung zum Datenschutzrecht an der Universität Zürich. Die Tagung stand unter dem Titel «Datenschutz – Kundendaten nutzen und schützen». Das Datenschutzrecht stellt insbesondere Unternehmen vor Herausforderungen. Denn sie möchten Kundendaten möglichst vielseitig nutzen können, während die Daten im Sinne der datenschutzrechtlichen Vorschriften zu schützen sind. Daraus entsteht ein Spannungsfeld. Der Schutz der Daten erweist sich als aufwendig, weil gesetzliche Regelungen eingehalten und mittels technischer Sicherheitsvorkehrungen umgesetzt werden müssen. Daher nimmt der Datenschutz im Unternehmensalltag meist nicht eine prominente Stellung ein. Kommt es jedoch zu Datenpannen, -missbräuchen oder -verlusten, kann dies einem Unternehmen enorme Reputationsschäden zufügen. Da bei strikter Einhaltung der Datenschutzvorschriften letztlich Wettbewerbsvorteile entstehen können, sind Unternehmen aufgrund wirtschaftlicher Überlegungen freiwillig zur Einhaltung der Anforderungen motiviert.

Der Datenschutz ist ein wichtiges Anliegen der schweizerischen Bevölkerung. Zu diesem Schluss kommt Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, aufgrund der

zum 3. Europäischen Datenschutztage vom 28. Januar 2009 in Auftrag gegebenen repräsentativen Umfrage.¹ Martina Arioli, LL.M., Rechtsanwältin in Zürich, begrüsst die Teilnehmenden und geht zur Einführung der Tagung auf die Ergebnisse der Umfrage ein. Drei Viertel der Befragten gaben an, dass es ihnen wichtig oder sehr wichtig sei, wie mit ihren persönlichen Daten im Internet umgegangen wird. Das fehlende Wissen erklärt den sorglosen Umgang mit Daten im Internet, was zu notorischem Missbrauch führt, folgert Privatim. Eine von zwei befragten Personen würde sich im Falle des Missbrauchs ihrer Daten an die Polizei oder ein Gericht wenden, 35% der Befragten an die datenmissbrauchende Organisation. Offensichtlich wird Datenmissbrauch als schwerwiegend eingeschätzt. Ein Fünftel der befragten Personen sieht die Privatsphäre in der Schweiz insgesamt ungenügend geschützt. Das Ergebnis der Umfrage zeigt zusammenfassend, dass die schweizerische Bevölkerung dem Schutz ihrer persönlichen Daten einen hohen Stellenwert einräumt und gleichzeitig wenig Wissen darüber hat, was mit ihren Daten wirklich geschieht. Thematisch interessant für die Tagung erweist sich die Erkenntnis, dass privaten Unternehmungen (Krankenkassen, Kreditkartenfirmen, Telekom-Anbieter) bezüglich des Umgangs mit Daten weniger Vertrauen geschenkt wird als öffentlichen Stellen (Polizei, Spitälern, Einwohnerämtern).

II. Erste Erfahrungen mit dem revidierten Datenschutzgesetz

Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) Hanspeter Thür zieht eine erste Bilanz zur Revision des Datenschutzgesetzes², welche am 1. Januar 2008 in Kraft getreten ist. Die wesentliche Idee der Gesetzesänderung war die Verbesserung der Transparenz bei der Datenbearbeitung.

Zu Beginn seines Referates geht Thür auf die Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten³ und Persönlichkeitsprofilen⁴ ein, welche im Rahmen der

¹ Die Ergebnisse der Umfrage sind abrufbar unter: www.privatim.ch.

² Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG), SR 235.1.

³ Zur Definition besonders schützenswerter Personendaten vgl. Art. 3 lit. c DSG.

⁴ Zur Definition von Persönlichkeitsprofilen vgl. Art. 3 lit. d DSG.

Revision mit Art. 7a DSG eingefügt wurde. Beispiele sind Surfgeohnheiten im Internet, Einkaufsverhalten oder Reiseaktivitäten. Es gibt Unternehmen, die Analysesoftware einsetzen, welche von den betroffenen Personen ein Profil erstellen. Damit können weitreichende Aussagen über eine Person gemacht werden, womit schnell die Grenze zu besonders schützenswerten Personendaten erreicht wird. In diesem Fall bestünde zwingend die Pflicht zur Information gemäss Art. 7a DSG. Daher empfiehlt der Referent die Anmeldung von solchen privaten Datensammlungen beim EDÖB gemäss Art. 11a Abs. 3 lit. a DSG.

Als weiteres Instrument der Förderung der Transparenz erwähnt der Referent die Pflicht der Erkennbarkeit der Datenbearbeitung für die betroffene Person. Art. 4 Abs. 4 DSG sieht neu diesen zentralen Grundsatz vor: Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen erkennbar sein. Falls der Betroffene nicht mit der Datenbearbeitung rechnen kann, muss der Datenbearbeiter informieren. Die Pflicht zur Information besteht auch bei der Änderung des Zwecks, falls diese nicht erkennbar ist. Die Information kann über eine Datenschutzerklärung oder die Allgemeinen Geschäftsbedingungen (AGB) erfolgen. Die physische Nähe zur Datenbeschaffung ist jedoch notwendig. Bei Daten aus allgemein zugänglichen Quellen (beispielsweise Telefonbuch) muss mit der Bearbeitung gerechnet werden – somit ist die Datenbearbeitung erkennbar. Werden damit jedoch Persönlichkeitsprofile erstellt, kann nicht mehr von der Erkennbarkeit der Datenbearbeitung ausgegangen werden. In einem solchen Fall muss informiert werden. Der Referent erwähnt zur Veranschaulichung der Problematik einige Anwendungsfälle aus der Praxis: So ist beispielsweise der «Mietercheck» ein Auskunftsservice, bei welchem online Bonitäts- und Wirtschaftsinformationen sowie ergänzende Informationen (Betreibungsauskünfte, Arbeitgeber- und Vermieterreferenzen) von Personen abgefragt werden können. Mit einer solchen Datenbearbeitung muss der Mieter nicht rechnen. Folglich müsste der Bearbeiter den Betroffenen informieren. Ausserdem ist in diesem Fall fraglich, ob es sich überhaupt um eine zulässige Datenbearbeitung handelt, denn den Vermieter darf nur die Solvenz interessieren.⁵

Bezüglich der grenzüberschreitenden Datenbekanntgabe hält *Thür* fest, dass gemäss Art. 6 DSG das fragliche Land einen angemessenen Datenschutz gewährleisten muss. Ist diese Voraussetzung nicht durch gesetzliche Regelungen erfüllt

und sollen die Daten dennoch weitergegeben werden, muss der EDÖB prüfen, ob hinreichende Garantien in anderer Form, beispielsweise in Vertragsklauseln oder zwischenstaatlichen Vereinbarungen, vorgesehen sind. Die Schweiz hat mit den USA ein Safe-Harbor-Abkommen unterzeichnet.⁶ Dieses Abkommen vereinfacht die Datenübermittlung von Unternehmen in der Schweiz zu Unternehmen in den USA und lässt die Meldepflicht bei EDÖB dahinfallen.⁷

Der Vortragende macht auf die neue Möglichkeit der Zertifizierung von Systemen, Verfahren oder der Organisation der Datenbearbeiter aufgrund einer Bewertung durch unabhängige Zertifizierungsstellen aufmerksam (Art. 11 DSG). Am 1. Januar 2008 ist die Verordnung über die Datenschutzzertifizierungen⁸ in Kraft getreten. Zertifizierte Unternehmen müssen ihre Datensammlungen dem EDÖB nicht melden (Art. 11a Abs. 5 lit. f DSG). Der EDÖB hat die Kompetenz, Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem zu erlassen (Art. 4 Abs. 3 VDSZ). Solche Richtlinien sind am 1. November 2008 in Kraft getreten. Aktuell akkreditiert die Schweizerische Akkreditierungsstelle (SAS) die Zertifizierungsstellen (Art. 1 VDSZ), welche künftig Zertifizierungen erteilen, sistieren oder entziehen werden (Art. 6 und 9 VDSZ). Der EDÖB ist Aufsichtsbehörde (Art. 10 VDSZ).

Mit einem Hinweis auf die grundsätzlich geltende Meldepflicht von Datensammlungen privater Personen beim EDÖB gemäss Art. 11a Abs. 3 DSG⁹ geht der Redner auf eine für Unternehmen wichtige Ausnahme ein: Von der Meldepflicht befreit wird unter anderem, wer einen unabhängigen Datenschutzverantwortlichen bezeichnet, der die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11a Abs. 5 lit. e DSG). Im letzten Jahr haben vor allem grössere und mittlere Unternehmen die Einsetzung eines internen Datenschutzbeauftragten gemeldet. Die unternehmensinternen Datenschutzbeauftragten haben sich in der Vereinigung der Unternehmensdatenschutzbeauftragten (VUD) zusammengeschlossen, welche mit dem EDÖB zusammenar-

⁶ Das Abkommen ist am 17. Februar 2009 in Kraft getreten.

⁷ Unternehmen in den USA können sich beim Handelsministerium der USA zur Einhaltung der im Abkommen festgehaltenen Datenschutzgrundsätze verpflichten und sich zertifizieren lassen. Schweizerische Unternehmen können Daten an diese zertifizierten Unternehmen übermitteln, ohne vorgängig Vertragsklauseln auszuhandeln oder den Vorgang dem EDÖB melden zu müssen.

⁸ Verordnung über die Datenschutzzertifizierungen vom 28. September 2007 (VDSZ), SR 235.13.

⁹ Das Anmeldeverfahren hat im November des letzten Jahres eine Neuerung erfahren, welche den Prozess vereinfacht. Neu können Anmeldungen von Datensammlungen via Internet unter folgender Adresse erfolgen: www.dataereg.admin.ch.

⁵ Die Empfehlung des EDÖB bezüglich dieses Falles ist abrufbar unter: www.edoeb.admin.ch (Informationsservice über Mieterbonität).

beitet. Aktuell betrifft die Diskussion dieser Vereinigung mit dem EDÖB die Anforderungen an die Unternehmensdatenschutzverantwortlichen und deren Ausbildung.

III. Schnittstellen und Reibungsflächen – Datenschutz im Unternehmensalltag

Bereits zu Beginn seines Referats macht *Christian Drechsler*, LL.M., Rechtsanwalt und Legal Counsel bei Zurich Financial Services in Zürich, auf die Wichtigkeit des Verhältnismässigkeitsgrundsatzes aufmerksam. Die wichtigste Schnittstelle zwischen Datenschutz und Unternehmensalltag ist der technische Datenschutz im IT-Bereich. Dies zeigt sich insbesondere beim Outsourcing (Computer-Support) und bei Hosting-Verträgen. Werden die Daten nur so bearbeitet, wie der Auftraggeber selbst es tun dürfte, und steht keine gesetzliche oder vertragliche Geheimhaltungspflicht entgegen, ist die Übertragung der Bearbeitung von Personendaten an Dritte zulässig (Art. 10a Abs. 1 lit. a und b DSGVO). Insbesondere ist darauf zu achten, dass der Dritte die erforderliche Datensicherheit gewährleistet (Art. 10a Abs. 2 DSGVO). Der Referent verdeutlicht die Problematik am Beispiel von Laptops. Der Passwortschutz auf einem Computer schützt nur das Gerät – nicht hingegen die Festplatte. Somit könnte bei einem Computer, welcher in die Hände eines Nichtberechtigten gerät, die Festplatte ausgebaut werden, ohne dass das Passwort einen Schutz gewähren würde. Auch der Fernzugriff (Remote Access), welcher meist bei IT-Wartungsverträgen vorgesehen wird, ermöglicht potenziell den Zugriff auf Personendaten. Um Schwierigkeiten zu umgehen, sollte als einfachste und sicherste Lösung auf den Fernzugriff verzichtet werden. Andernfalls sollten vertragliche Zusicherungen bestehen, welche die Sicherheit der Daten gewährleisten.

Als zweite Schnittstelle erwähnt der Redner die Kommunikation, insbesondere bei Datenverlust oder -diebstahl. Statistisch errechnet, tritt in jedem Unternehmen alle drei Jahre der Verlust von Daten auf. Bei einem solchen Vorfall besteht grundsätzlich keine Rechtspflicht zur Information. Aufgrund des Risikos der Schädigung des Ansehens werden jedoch die meisten Unternehmen ein Interesse zeigen, den Zwischenfall aufzuklären und die Angelegenheit zu melden. Ausschlaggebend ist bei einem Vorkommnis, dass strategisch richtig verfahren wird und die Abläufe gut vorbereitet sind. Der Datenverlust bei Vertragspartnern – beispielsweise beim Outsourcing – sollte im Vertrag geregelt werden.

Der Vortragende nennt weitere Schnittstellen innerhalb des Datenschutzgesetzes. Diese beste-

hen, weil in diesem Gesetz das Privatrecht und das öffentliche Recht nicht systematisch voneinander abgegrenzt werden. Ein Beispiel zur Veranschaulichung ist Art. 6 DSGVO. Dessen Abs. 1 und 2 enthält Privatrecht, während Abs. 3 dem öffentlichen Recht zuzuordnen ist. Insgesamt handelt es sich bei den Bestimmungen im Datenschutzgesetz vor allem um Privatrecht mit der Ausnahme der Bestimmungen, die den Bund betreffen.

Abschliessend spricht *Drechsler* über Reibungsflächen. Einerseits lassen sich diese im Zusammenhang mit anderen Rechtsgebieten finden. Das Risikoprofil ist in den verschiedenen Rechtsgebieten unterschiedlich. Beim Datenschutzrecht ist jede betroffene Person einem potenziellen Risiko der rechtswidrigen Datenbearbeitung ausgesetzt, während in anderen Rechtsgebieten nur ein beschränkter Personenkreis vom Risiko betroffen ist. Somit besteht eine grosse Anzahl potenzieller Kläger.

Andererseits stellen die Theorie und die Praxis eine Reibungsfläche dar. In der Praxis stellt die Umsetzung des Schutzes von Daten oft eine Schwierigkeit dar, denn es werden unzählige Daten aufgrund von Vertraulichkeitsklauseln übermittelt. Zudem sind bei konzernweiten Datentransfers oftmals keine Datenschutzverträge vorgesehen. Daher ist es essenziell, die Wichtigkeit und die Besonderheit des Datenschutzes zu kommunizieren und bewusst zu machen.

IV. Die Bearbeitung von Personendaten zu Marketingzwecken – «the dos and don'ts»

Einleitend umschreibt Dr. *Jürg Schneider*, Rechtsanwalt bei Walder Wyss & Partner AG in Zürich, den Begriff Marketing: Marketing sind Aktivitäten zur Schaffung, Kommunikation und Lieferung von Angeboten, die einen Wert für den Kunden schaffen. Die Verwendung von Personendaten ermöglicht ein effizienteres Marketing. Grundrechtlich ist das Betreiben von Marketing durch die Wirtschaftsfreiheit nach Art. 27 BV geschützt. Dieses Grundrecht gilt jedoch nicht absolut und wird durch das Grundrecht auf informationelle Selbstbestimmung beschränkt, welches in Art. 13 Abs. 2 BV gewährleistet wird. Somit ergibt sich ein Spannungsverhältnis zwischen Marketing und Datenschutz.

Nach allgemeinen Ausführungen zum Datenschutzgesetz geht der Referent auf die Beschaffung von Personendaten zu Marketingzwecken ein. Diese ist grundsätzlich möglich und nicht verboten. Dabei müssen die Grundsätze und Anforderungen des Datenschutzgesetzes eingehalten werden. Die Verwendung der Adresse von bereits

bestehenden Kunden zu Marketingzwecken für eigene Produkte ist gestattet. Wünscht der Kunde ausdrücklich keine solche Nutzung, ist diese nicht zulässig. Der Kunde muss dies jedoch mitteilen, andernfalls ist die Verwendung erlaubt. Hier stellt sich die Frage, ob ein Eintrag in der Robinsonliste genügt. Gemäss dem Referent darf das Unternehmen den Kunden anschreiben, selbst wenn ein Eintrag in der Liste vorhanden ist. Erst wenn der Kunde mitteilt, dass er keine Werbung wünscht, darf ihn das Unternehmen nicht mehr anschreiben. Kundenadressen dürfen nicht für Drittwerbung genutzt werden oder an Dritte weitergegeben werden. Eine Ausnahme liegt vor, wenn der Kunde vorgängig klar informiert wurde und (mindestens) stillschweigend eingewilligt hat. Wettbewerbe und andere Verkaufsförderungsmaßnahmen bedingen die transparente Information der Betroffenen und erfordern ihre Einwilligung. Die Erwähnung in den AGB reicht aus – es braucht kein Kästchen zum Ankreuzen.

Schneider macht darauf aufmerksam, dass seit dem 1. April 2007 eine gesetzliche Grundlage für Massenwerbung besteht. Massenwerbung ist die automatische Werbung ohne menschlichen Aufwand. Das Datenschutzgesetz und das Bundesgesetz gegen den unlauteren Wettbewerb¹⁰ sind parallel anwendbar. Gemäss Art. 3 lit. o UWG handelt insbesondere unlauter, wer Massenwerbung ohne direkten Zusammenhang mit einem angeforderten Inhalt fernmeldetechnisch sendet, ohne vorher die Einwilligung des Kunden einzuholen, den korrekten Absender anzugeben oder auf eine problemlose und kostenlose Ablehnungsmöglichkeit hinzuweisen. Nicht unlauter handelt hingegen, wer beim Verkauf von Waren, Werken oder Leistungen die Kontaktinformationen vom Kunden erhalten hat, den Kunden dabei auf die Ablehnungsmöglichkeit hingewiesen hat und diesem Kunden ohne dessen Einwilligung nur Massenwerbung für eigene ähnliche Waren, Werke oder Leistungen sendet. Letztere Voraussetzungen müssen kumulativ erfüllt sein.

Der Vortragende spricht in der Folge über Kundenbindungsprogramme, Data Mining und Scoring als weitere Marketingmittel. Bei diesen Mitteln werden in der Regel Persönlichkeitsprofile geschaffen. Der Persönlichkeitsschutz muss gewährleistet werden, und die allgemeinen Grundsätze müssen eingehalten werden. Bei Kundenbindungsprogrammen werden Kundenvorteile (beispielsweise Rabatte oder Prämien) gegen die Einwilligung zur Auswertung von Kundendaten zu

Marketingzwecken erteilt. Besonders wichtig sind auch hier die transparente Aufklärung der Kunden und die Einhaltung der Zweckbestimmung. Berühmte Beispiele sind die Kundenbindungsprogramme der Migros-«Cumulus-Karte» sowie die «Coop-Supercard». Beim Data Mining werden Daten aufgespürt und kombiniert, um neue, noch unbekannte Personendaten zu erzeugen. In diesem Zusammenhang zeigt sich die Problematik einerseits beim Zweckbindungsgebot, andererseits bezüglich der Einwilligung als Rechtfertigungsgrund. Zur Risikominimierung wird die präzise Information der Kunden, die kontinuierliche Überprüfung der Zweckbindung oder das Vorsehen eines «Opting-out» für die Kunden empfohlen. Beim Scoring wird eine Prognose des zukünftigen Verhaltens von Personen mit bestimmten Merkmalen gestellt. Die Einwilligung ist notwendig, sofern mehr als nur die Kreditwürdigkeit geprüft wird. Es muss Auskunft erteilt werden über Rohdaten, deren Herkunft, Interpretation, errechnete Scores und den Empfänger. Das Verhältnismässigkeitsgebot ist besonders zu beachten bei der Gewichtung der Kriterien.

Abschliessend fasst *Schneider* die «dos» und «don'ts» zusammen. Wichtigstes Gebot ist die Information der betroffenen Personen. Der Bearbeitungszweck ist klar zu umschreiben. Insbesondere ist die Weitergabe der Daten an Dritte mitzuteilen und die Einwilligung der betroffenen Person einzuholen, wo dies notwendig ist. Wird Massenwerbung betrieben, muss Art. 3 lit. o UWG beachtet werden. Besondere Marketingmittel, wie Kundenbindungsprogramme, Data Mining und Scoring sind datenschutzrechtskonform auszugestalten. Bezüglich der «don'ts» hält der Referent im Umkehrschluss die Datenbearbeitung ohne ausreichende Information der betroffenen Personen, die Bekanntgabe an Dritte ohne ihre Einwilligung oder die Bearbeitung gegen ihren ausdrücklichen Willen fest. Ebenso ist eine Datenspeicherung auf Vorrat zu vermeiden.

V. Risikomanagement im Datenschutz – Grundsätzliches und Lessons Learned aus den jüngsten Datenschutzvorfällen

Dorothee Schrief, Leiterin bei der Deutschen Telekom-Gruppe in Bonn, macht nach einleitenden Bemerkungen zunächst auf die Risiken für das Unternehmen aufmerksam, welche aus der Nichterfüllung von aufsichtsbehördlichen Auflagen oder Kundenforderungen resultieren können: Strafverfolgung, Reputationsschaden, Investitionsfehler, Business-Continuity-Risiko sowie das Risiko der Selbstverstärkung. Um diese Risiken zu minimie-

¹⁰ Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (UWG), SR 241.

ren, sind zur Qualitätssicherung Vorgänge in verschiedenen Bereichen der Unternehmung notwendig. Vier Teile tragen zur Qualitätssicherung und damit zum Erreichen des verfolgten Ziels bei, welches die Minimierung von Risiken und die Gewährleistung eines angemessenen Datenschutzniveaus ist. Der erste Teil ist die Umsetzung. Dahin gehören der technische Datenschutz, Schulungen usw. Die Organisation ist ein weiterer Teil. In diesem Zusammenhang geht es insbesondere um Zugangspläne. Das Berichtswesen – als dritter Teil – garantiert eine effiziente Kontrolle bei Einzelfällen oder in regelmässigen Abständen (beispielsweise wöchentlich oder monatlich). Als vierter und letzter Teil muss dafür gesorgt werden, dass Richtlinien – zum Beispiel der Datenschutzverhaltenskodex oder das Mitarbeitendenhandbuch – erstellt und an die Mitarbeitenden kommuniziert werden. Unternehmen sollten ein strukturiertes, qualitätsorientiertes Datenschutz-Managementsystem einrichten, mindestens mit den Bereichen Organisation, Regulierung, Implementierung sowie Kontrolle.

Die Vortragende hebt hervor, dass die Datenschutzorganisation Mehrwert für das Unternehmen generieren kann. Aufgrund der Dokumentation von Verfahren und Anwendungen werden IT-Anwendungen von Beginn weg konform ausgestaltet, entsteht weniger Nachbesserungsbedarf, und die Qualität von Arbeitsergebnissen steigt. Durch die rechtzeitige Einbeziehung von Datenschutzregeln können für die Unternehmung Kosten und Reputationsschäden oder Imageverluste vermieden werden. Auch unternehmensintern können Spannungen verringert und die Motivation der Mitarbeitenden gesteigert werden. Insgesamt bringt somit ein gut funktionierendes Datenschutzsystem einen Wettbewerbsvorteil für ein Unternehmen mit sich – insbesondere wenn beispielsweise Zertifizierungen oder Qualitätssiegel eingeführt werden oder die Unternehmung damit in der Lage ist, Vertrauen bei den Kunden zu erwecken.

Abschliessend erläutert die Referentin die gezogenen Lehren aus den Geschehnissen bei der Deutschen Telekom.¹¹ Zur Vermeidung von Datenmissbrauch muss der IT-Sicherheit eine stärkere Position eingeräumt werden, sollten die Zugangsbefugnisse stärker geregelt werden, der Benutzerauthentifizierung als auch der Kundenidentifizierung hohes Gewicht beigemessen werden, alle Vorgänge immer überwacht und protokolliert wer-

den und die beteiligten Personen sensibilisiert werden (beispielsweise durch entsprechende Regelungen in Verträgen). Da nicht alles kontrolliert werden kann, erweist sich das Vorbereitetsein auf den Ernstfall als die beste Massnahme.

VI. Internetdienste und Datenschutz

Per Meyerdierks, Beauftragter für den Datenschutz und Justitiar bei der Google Germany GmbH in Hamburg, stellt in seinem Referat die Frage: Sind IP-Adressen personenbezogene Daten? Zu Beginn geht der Referierende auf technische Abläufe ein. Ein Internetnutzer braucht für die Nutzung des Internets einen Anschluss. Ein Access-Provider ermöglicht ihm aufgrund eines Vertragsverhältnisses den Anschluss und weist ihm bei jeder Einwahl in das Internet eine IP-Adresse zu. Werden im Internet Webseiten besucht, übermittelt der Computer die IP-Adresse an den Betreiber der Webseite. Webseitenbetreiber setzen Webserver ein, welche die Daten einer Webseite speichern und Datenabfragen von Computern beantworten. Gleichzeitig werden meist die IP-Adresse und der Zeitpunkt des Besuches der Webseite aufgezeichnet und in einem Serverlog eingetragen und gespeichert.

Meyerdierks beschreibt zunächst die Rechtslage in der EU, in Deutschland und in der Schweiz und vergleicht diese. Das europäische Datenschutzrecht sieht in Art. 7 der EU-Datenschutzrichtlinie¹² ein «Verbot mit Erlaubnisvorbehalt» vor. Das heisst, dass alles, was Datenbearbeitung betrifft, grundsätzlich verboten ist. Dies gilt somit auch im deutschen Recht zum Datenschutz¹³. Im schweizerischen Recht gilt der umgekehrte Grundsatz. Grundsätzlich ist die Datenbearbeitung erlaubt, es sei denn, sie ist verboten. Dem Art. 7 EU-Datenschutzrichtlinie entspricht in der Schweiz in etwa der Art. 13 Abs. 1 DSG. Würde man IP-Adressen als personenbezogene Daten betrachten, stünde möglicherweise eine Verletzung des Persönlichkeitsrechts gemäss Art. 12 Abs. 2 lit. a i.V.m. Art. 4 Abs. 4 DSG durch das Betreiben einer Webseite im Raume. In Deutschland wäre die Betreibung einer Webseite verboten. Weil sich im

¹² Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG, EU-Datenschutzrichtlinie), ABI L 281 vom 23.11.1995, S. 31–50.

¹³ § 4 Abs. 1 BDSG (Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003, BGBl. I S. 66, zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006, BGBl. I S. 1970).

¹¹ In den letzten zwei Jahren wurden bei der Deutschen Telekom unzählige Daten entwendet. Die Ermittlungen diesbezüglich sind im Gange.

Telemediengesetz¹⁴ jedoch eine gesetzliche Grundlage findet, ist die Bearbeitung zulässig.

Der Redner beantwortet die Frage, ob IP-Adressen personenbezogene Daten sind, aus den verschiedenen Blickwinkeln anders. Da der Access-Provider über Angaben mindestens bezüglich Namen und Anschrift des Kunden verfügt, handelt es sich aus Sicht des Access-Providers um personenbezogene Daten. Aktuell ist eine Diskussion im Gange, welche die Frage zu beantworten versucht, ob in einem Serverlog des Webseitenbetreibers gespeicherte IP-Adressen personenbezogene Daten sind. Es stehen sich zwei Meinungen gegenüber. Einerseits wird der objektive Begriff der Personenbeziehbarkeit vertreten, wonach die theoretische Möglichkeit der Herstellung eines Personenbezugs ausreicht, um den Personenbezug des Datums zu bejahen. Die Ansicht des relativen Personenbezugs zieht nur die Verhältnisse der verarbeitenden Stelle ein und lässt Kenntnisse und Fähigkeiten Dritter ausser Acht. Es geht nur um die Bestimmbarkeit der Person hinter der IP-Adresse für die verarbeitende Stelle selbst.

Die beiden Theorien führen zu unterschiedlichen Antworten auf die Frage bezüglich der Personenbeziehbarkeit von IP-Adressen, wie der Referent darlegt. Bei IP-Adressen an sich und der mit

ihnen gespeicherten Zeitangabe handelt es sich nicht um personenbezogene Daten, da es an der Bestimmbarkeit der Person fehlt. Wurde die IP-Adresse gleichzeitig im Log des Access-Providers gespeichert, kann der Access-Provider auf die Schlüsseldaten (Namen, Anschrift) zurückgreifen. Somit könnte der Eintrag im Serverlog einem Anschlussinhaber zugeordnet werden. Vertritt man den objektiven Begriff der Personenbeziehbarkeit, werden die sich beim Access-Provider befindenden Schlüsseldaten miteinbezogen und somit die Personenbezogenheit von IP-Adressen bejaht. Bei der entgegengesetzten Meinung steht der relative Personenbezug im Vordergrund, weshalb die Schlüsseldaten nicht miteinbezogen werden und somit die Personenbezogenheit von IP-Adressen verneint wird.

Meyerdierks vertritt die Meinung des relativen Personenbezugs und kommt somit zum Schluss, dass IP-Adressen keine personenbezogenen Daten sind. Als Argumente führt er an, dass der Webseitenbetreiber keine Verbindung zum Access-Provider herstellen kann und es dem Access-Provider nicht erlaubt ist, die Daten bekannt zu geben. Nur wenn dies praktisch möglich und rechtlich zulässig wäre, würden Personendaten vorliegen.

¹⁴ § 15 Abs. 1 TMG (Telemediengesetz vom 26. Februar 2007, BGBl. I S. 179, geändert durch Artikel 2 des Gesetzes vom 25. Dezember 2008, BGBl. I S. 3083).