# Newsletter
## #01 / 2017

Liebe Leserin, lieber Leser

«Digitalisierung und Schutz der Privatsphäre»: Das Thema des 10. Schweizerischen Datenschutzrechtstags setzt sich auseinander mit dem, was Gilles Babinet, Unternehmer und Frankreichs Vertreter für digitaltechnische Fragen bei der EU-Kommission in Brüssel, in einem Artikel über das digitale Zeitalter schreibt, das er als radikalen Paradigmenwechsel für die Menschheit sieht («L'ère numérique, un nouvel âge pour l'humanité»). So sind die Unmengen an weiterverbreitetem Wissen und technischem Know-how im Gesundheitswesen, das Aufkommen der Robotertechnik und die Redimensionierung der Staaten einige Stichworte für das, was den Lauf der Menschheitsgeschichte ändern wird.

Bezeichnenderweise ist im digitalen Zeitalter der Zugang zu Informationen so einfach wie noch nie und kostet kaum etwas. Gilles Babinet nennt als Beispiel den Vergleich zwischen einem Quantenphysiker, der sich in der Welt der Wissenschaft bewegt, und einem Bauern, der in einer abgelegenen Region in Guatemala lebt. Eigentlich haben beide gleichermassen Zugang zu Informationen; was sie unterscheidet ist die Möglichkeit, das Informationsangebot zu nutzen, die Information an sich ist aber da. Der Kulturjournalist Alexandre Demidoff hat dies in einem Artikel über das Teilen von Wissen im digitalen Zeitalter auf den Punkt gebracht («A l'ère numérique, l'érudit sait partager son savoir»).

Wir müssen uns insbesondere fragen, was sich für uns mit der Digitalisierung alles ändern wird und wie gross die Gefahr für unsere Privatsphäre ist. Die äusserst interessanten Referate, die am 2. Juni an der Universität Freiburg gehalten worden sind, haben sowohl zum Nachdenken angeregt, als auch Lösungsansätze aufgezeigt. Meiner Ansicht nach wird die digitale Revolution sicher schneller verlaufen als jede andere, und wir müssen daher ganz besonders wachsam sein.

Besondere Aufmerksamkeit ist diesem Phänomen deshalb zu schenken, weil es sich auf grenzenlose Bereiche erstreckt, wie das Bildungswesen, das Gesundheitswesen, die Wirtschaft und sogar den Staat. Fast alles kann digitalisiert werden. Beste Beispiele dafür sind etwa die digitalen Bildungsangebote mit den sogenannten MOOCs (massive open online course), also allgemein zugängliche Online-Lernplattformen, die genetische Sequenzierung oder DNA als Schlüsselparameter, die Automatisierung und Robotertechnik, die in immer mehr Unternehmen zum Einsatz kommen, oder auch digitale Systeme mit Einsatzmöglichkeit in der inneren oder äusseren Sicherheit, Geldausgabe, Städteplanung usw.

In Anbetracht dieser Herausforderung muss die Privatsphäre unbedingt geschützt werden. Die Gesetzgebung muss diesbezüglich nicht nur genügend klar sein, sondern auch rasch angepasst werden können, um nicht ins Hintertreffen zu geraten.

Ich wünsche Ihnen eine angenehme Lektüre.

Laurent Schneuwly, Präsident der kantonalen
Öffentlichkeits- und Datenschutzkommisson

ETAT DE FRIBOURG
STAAT FREIBURG

**Autorité cantonale de la transparence et de la protection des données** ATPrD
**Kantonale Behörde für Öffentlichkeit und Datenschutz** ÖDSB

EC 902

# Inhalt



# Aktualitäten

## Digitalisierung und Schutz der Privatsphäre

*Am Zehnten Schweizerischen Datenschutzrechtstag Anfang Juni in Freiburg wurde das Thema «Digitalisierung und Schutz der Privatsphäre» aus unterschiedlichen Blickwinkeln betrachtet. Zur Sprache kamen sowohl die aus der Digitalisierung folgenden aktuellen Herausforderungen für das Datenschutzrecht als auch diejenigen für das Vertragsrecht.*

«Wenn auch die Wahl des Themas banal ist, so ist es das Thema an sich keinesfalls», erklärte der Eidg. Datenschutz – und Öffentlichkeitsbeauftragte, Adrian Lobsiger, zu Beginn der Tagung. Die Digitalisierung stelle vielmehr einen Lebensstil dar, der uns alle erfasse. Sie sei ein Geschäftsmodell, an dem alle teilhaben wollten – natürlich auch die Schweiz. So bleibe gar keine andere Wahl, als das Thema anzupacken und darauf Einfluss zu nehmen, auch wenn wir von der Entwicklung überrascht worden seien.

### «Wir müssen dringend handeln»

Wir seien an einem Moment angekommen, an dem der Mensch und das Menschliche keine Bedeutung mehr habe, sondern nur noch Daten, gab Dirk Helbling, Professor an der ETH Zürich zu bedenken. So liessen sich gesammelte Daten beispielsweise zur Wählerbeeinflussung nutzen. Er zitierte eine Firma, die mit einer neuen Methode Menschen anhand ihrer Facebook-Profile minutiös analysiere und somit Politikern zum Sieg verhelfe.

Bald könne dieses Modell anhand von zehn Facebook-Likes eine Person besser einschätzen als ein durchschnittlicher Arbeitskollege. 70 Likes reichten, um die Menschenkenntnis eines Freundes und 150 um die der Eltern zu überbieten. «Mit 300 Likes kann die Maschine das Verhalten einer Person eindeutiger vorhersagen als deren Partner», erklärte Helbling.

Die Menschheit müsse dringend handeln. Einerseits gebe es Riesenlöcher in den Datenschutzgesetzgebungen, die gestopft werden müssen. Andererseits müsse auch die Kontrolle über unseren Planeten auf partizipative Art und Weise verteilt werden. Ansonsten drohe die Kontrolle verloren zu gehen.

### Gedanken über die staatlichen Institutionen

In einem Bereich, in dem ein immer rascherer Wandel stattfindet, besteht für die Juristen auf institutioneller Ebene Handlungsbedarf. Gemäss Bertil Cottier, Professor an der Universität der italienischen Schweiz, kann das Legalitätsprinzip, wonach das Recht Grundlage und Grenze des Staates ist, der Unvorhersehbarkeit und der

Unsicherheit im Zuge der Digitalisierung nicht standhalten. Der Gesetzgeber läuft Gefahr, diesbezüglich den Anschluss zu verlieren, denn es braucht eine gewisse Zeit, um den Gesetzgebungsprozess in Gang zu setzen. Schuld daran sind zum Teil auch ungeeignete und zu lange Verfahren. Es herrscht also eine grosse Rechtsunsicherheit.

Bertil Cottier erklärte auch, dass die partizipativen Instrumente, die den privaten Unternehmen einen gewissen Spielraum lassen, zu ihrem Vorteil genutzt werden, damit diese nicht Opfer restriktiver Massnahmen seitens des Staates werden. Dieses Phänomen hat die Juristen veranlasst, sich neuen gesetzgeberischen Mechanismen zu widmen. Eine Lösung wären die Empfehlungen der guten Praxis, die im Vorentwurf des Datenschutzgesetzes beschrieben werden und von der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten verfasst oder genehmigt werden können. Leider sind sie aber nicht verbindlich. Der Referent schlug deshalb die Bildung einer unabhängigen, für den Datenschutz verantwortlichen Kommission vor, die verbindliche Empfehlungen erlassen könnte.

Im gleichen Sinne regte der stellvertretende Eidg. Datenschutz- und Öffentlichkeitsbeauftragte Jean-Philippe Walter an, die Gesetze sollten weniger ins Detail gehen und die Datenschutzbeauftragten mehr Handlungsfreiheit haben, um sich der Tag für Tag stattfindenden Entwicklung anzupassen. Er sprach sich auch dafür aus, die Technologie zu nutzen, die nicht nur negative Seiten hat, und gab zu bedenken, dass wir ohne Neuerung den Geschäftsmodellen gegenüber ins Hintertreffen geraten werden. Gemäss Thomas Probst, Professor an der Universität Freiburg, enthalten die Bestimmungen des Obligationenrechts alle notwendigen Normen, um sich den Herausforderungen der Digitalisierung zu stellen. Das Problem liegt ihm zufolge nicht so sehr im Inhalt des Gesetzes, sondern vielmehr in dessen richtigen Anwendung, insbesondere in der Garantie der Grundprinzipien, wie der Einwilligung nach angemessener Information.

So vielfältig die in den Referaten und Workshops behandelten Themenbereiche waren, so einig waren sich die Referenten und Tagungsteilnehmer: Die Digitalisierung stellt uns vor einige Herausforderungen und immer komplexere Probleme. Es ist aber noch nicht zu spät für konkrete und dynamische Massnahmen.

## Überwachung des Post- und Fernmeldeverkehrs

—

Das neue Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs soll ein Gleichgewicht zwischen Überwachung und Privatsphäre schaffen. Es gilt nur unter restriktiven Voraussetzungen und im Rahmen eines Strafverfahrens, zum Vollzug eines Rechtshilfeersuchens, im Rahmen der Suche nach vermissten Personen oder im Rahmen der Fahndung nach verurteilten Personen. Das Gesetz sieht zwei verschiedene Arten der Datenbeschaffung vor, und zwar mit Überwachung in Echtzeit, bei der der Inhalt der Kommunikation umgeleitet wird, und mit rückwirkender Überwachung. Dazu können IMSI-Catcher eingesetzt werden, die sich als Mobilfunkantennen tarnen und die Mobilfunkgeräte ausspähen, die sich verbinden. Eine zweite Möglichkeit ist der Einsatz von GovWare, sogenannten Staatstrojanern, mit denen in Computern Überwachungssoftware installiert werden kann. Eine weitere Neuerung ist das vom Dienst Überwachung Post- und Fernmeldeverkehr kontrollierte IT-System für eine effizientere Datenverwaltung, insbesondere für eine sicherere Übermittlung dieser Daten an die Behörde, die die Überwachung beantragt hat.

Véronique Jaquet, Rechtsanwältin und wissenschaftliche Mitarbeiterin beim Bundesamt für Justiz brachte jedoch am Schweizerischen Datenschutzrechtstag ihr Bedauern darüber zum Ausdruck, dass die Gesetzgebungsarbeit aus dem Jahr 1990 gegenüber den technologischen Fortschritten ins Hintertreffen geraten ist. Nach dem Gesetz ist also keine Überwachung verschlüsselter Kommunikation im Internet möglich. Daher kommt eine Überwachung von WhatsApp nicht in Frage. Die Parlamentarierinnen und Parlamentarier waren ausserdem geteilter Meinung in Bezug auf die Einhaltung des Datenschutzes. Einige begrüssten die dafür vorgesehenen Rahmenbedingungen, andere waren der Ansicht, es wäre besser, das Bestehende auszubauen, hauptsächlich die Strafprozessordnung, und nicht den Nachrichtendienst, der im Verborgenen arbeiten sollte, mit mehr Macht auszustatten und somit seine Tätigkeit mit der Möglichkeit von Rechtsmitteln sichtbarer zu machen.

## Datenschutz im Arbeitsrecht

*Das Centre d'étude des relations de travail (CERT) führte eine Tagung zu den Neuerungen, die 2016 im Arbeitsrecht eingetreten sind, und dem Datenschutz in diesem Bereich durch. Die Referenten befassten sich insbesondere mit Fragen zum Datenschutz im Rekrutierungsverfahren, zum Schutz medizinischer Daten, die Versicherern mitgeteilt werden, sowie zum Schutz digitaler Daten. Das Bundesamt für Justiz stellte den Vorentwurf der Reform der eidgenössischen Datenschutzgesetzgebung vor, mit einem kurzen Überblick über den diesbezüglichen internationalen Kontext. Der stellvertretende Eidg. Datenschutz- und Öffentlichkeitsbeauftragte sprach über den Zugang zu amtlichen Dokumenten. Zu diesem Thema ist auch eine Publikation von Jean-Philippe Dunand und Pascal Mahon mit dem Titel «La protection des données dans les relations de travail» herausgegeben worden.*

Jeder Arbeitgeber beschafft im Rekrutierungsverfahren zahlreiche auf die Stellenbewerber bezogene Personendaten und bearbeitet sie. Dieses Bearbeiten von Personendaten kann zu Persönlichkeitsverletzungen führen und für die betreffenden Personen auch ein Diskriminierungsrisiko bergen. In der Schweiz sind diese Aspekte in verschiedenen Rechtsnormen geregelt. Tatsächlich wird das grundrechtliche Diskriminierungsverbot (Art. 8 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999; BV) mit zwei Bundesgesetzen über die Gleichbehandlung umgesetzt (Bundesgesetz über die Gleichstellung von Frau und Mann vom 24. März 1995 und Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderung vom 13. Dezember 2002), das Bundesgesetz über den Datenschutz vom 19. Juni 1992 trägt insbesondere zur Umsetzung des Rechts auf Schutz der Privatsphäre bei (Art. 13 BV), und das Recht, im Rahmen des Arbeitsverhältnisses nicht widerrechtlich in seiner Persönlichkeit verletzt zu werden, ist im Obligationenrecht (OR) vom 30. März 1911 festgeschrieben.

Karine Lempen, Professorin an der Rechtsfakultät der Universität Genf, befasste sich mit der Art und Weise, wie das Antidiskriminierungsrecht mit den Persönlichkeits- und Datenschutznormen in einem Anstellungsverfahren interagiert. Im Auswahlverfahren darf der Arbeitgeber Daten über den Arbeitnehmer bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind (Art. 328 und 328b OR). Der Referentin zufolge verfolgen die drei vorerwähnten Regelungen ähnliche Ziele und sehen grösstenteils dieselben Daten als «sensibel» an. Unter Vorbehalt beispielsweise der Umsetzung positiver Massnahmen zur beruflichen Eingliederung gewisser untervertretener gesellschaftlicher Gruppen erlauben das Antidiskriminierungsrecht sowie die Datenschutzgesetzgebung die Bearbeitung besonders schützenswerter Daten bei der Rekrutierung nur sehr begrenzt. So ergänzen und verstärken sich Datenschutz und Diskriminierungsschutz im Anstellungsverfahren gegenseitig.

### Schutz von Versicherern gemeldeten Daten

Das Sozial- und Privatversicherungswesen gehört zweifellos zu den Tätigkeitsbereichen, die das grösste Datenvolumen generieren. Diese Daten sind meist sehr sensibel, soweit sie sich auf den Gesundheitszustand der versicherten Personen beziehen. Anne-Sylvie Dupont, Professorin an den Universitäten Neuenburg und Genf, sprach über die Datenbearbeitung durch die Versicherer nach Beantragung einer Versicherungsleistung.

Um in Kenntnis der Sachlage entscheiden zu können, muss der Versicherer eine gewisse Anzahl personenbezogener Daten über die versicherte Person zusammentragen, bei denen es sich grösstenteils um sensible Daten handelt. Nach den allgemeinen Vorschriften zum Schutz sensibler medizinischer Daten dürfen die Daten an niemanden weitergegeben werden, sofern die versicherte Person der Bekanntgabe nicht zustimmt, keine gesetzliche Bestimmung die Datenübertragung erlaubt oder auch kein anderer Rechtfertigungsgrund für die Informationsübermittlung besteht. Professorin Dupont zufolge könnte man auf den ersten Blick meinen, es sei schwierig für den Versicherer, an die Daten über die versicherten Personen zu kommen. Bei der Beantragung von Versicherungsleistungen sind jedoch die Versicherten für die Versicherer praktisch «gläserne Menschen», die sich ihren Aufforderungen nach Preisgabe von Informationen kaum widersetzen. Das liegt insbesondere am Kräfteverhältnis zwischen den versicherten Personen, die meistens auf die Versicherungsleistungen angewiesen sind, um über die Runden zu kommen, und den Versicherern, die am Geldhahn sitzen und sich alle Zeit nehmen können, um genau abzuklären, ob eine Auszahlung wirklich gerechtfertigt ist.

Die Referentin gab auch zu bedenken, dass die von einer Sozialversicherung oder einer Privatversicherung gesammelten Informationen anderen Versicherungen und gewissen

Verwaltungsbehörden leicht zugänglich sind, insbesondere im Hinblick auf die Mitwirkungspflicht der versicherten Person, die Leistungen beantragt hat. Mit der Zustimmung, ihre Daten einem Versicherer mitzuteilen, muss die versicherte Person damit rechnen, dass diese Daten noch vielen anderen Beteiligten zur Verfügung gestellt werden können; sie kann aber nicht im Voraus wissen, wem diese Daten dann zugänglich gemacht werden, weil die gesetzliche Regelung kompliziert ist und meistens keine diesbezügliche Vorinformationspflicht besteht. Die Zahl der Personen, die Kenntnis ihrer Personendaten erlangen könnten, ist somit exponentiell.

Professorin Dupont äusserte zum Schluss ihre Ansicht, wonach eine klare Trennung zwischen den Leistungen und dem Arztbericht sowie eine Sensibilisierung der von den Versicherungen eingesetzten Gutachter für den Grundsatz der Verhältnismässigkeit dem Schutz der Versichertendaten Vorschub leisten würde.

## Berufsgeheimnis bei Patientendaten

—

*«Hat das Berufsgeheimnis noch eine Zukunft?» Dies war Thema der öffentlichen Veranstaltung von privatim anlässlich des Frühlingsplenums vom 17. Mai 2017 in Schaffhausen.*

Viele Ärzte, Spitäler und Institute lagern die elektronische Verwaltung, Archivierung und Bearbeitung ihrer Patientendaten aus. Immer öfter werden dazu auch Cloud-Lösungen eingesetzt. Wolfgang Wohlers, Professor für Strafrecht an der Universität Basel, hat zum Outsourcing von patientenbezogenen Gesundheitsdaten ein Gutachten erstattet. Er kommt darin zum Schluss, dass ein Outsourcing mit dem Patientengeheimnis nicht vereinbar ist. IT-Dienstleistungserbringer und Clouddienste könnten aufgrund ihrer wirtschaftlichen Selbständigkeit und des fehlenden Unterordnungsverhältnisses nicht einfach als «Hilfspersonen» des Arztes oder Spitals qualifiziert werden. Es liege auch nicht im Belieben des Dienstleistungserbringers, ohne Einwilligung des Geheimnisherrn, z.B. des Patienten, den Kreis der Geheimnisträger bzw. der «zum Wissen Berufenen» auszuweiten. Vielmehr sei es der Patient, der entscheide, mit wem er sein Wissen teile. Eine Ausweisung dieses Kreises verletze daher das Berufsgeheimnis nach Art. 321 und Art. 321bis StGB.

### Lockerung des Patientengeheimnisses?

Das Thema der Auslagerung wurde unter verschiedenen Aspekten thematisiert. Hanspeter Kuhn, Vertreter der Verbindung der Schweizer Ärztinnen und Ärzte, zeigte anhand verschiedener Beispiele auf, wie das Patientengeheimnis in der Vergangenheit gelockert worden ist. So sehen verschiedene Gesetzesbestimmungen Mitteilungspflichten vor, so zum Beispiel an Krankenversicherer, an das Bundesamt für Gesundheit oder an das Krebsregister. Outsourcing sei gelebte Wirklichkeit; ohne Arbeitsteilung sei eine effiziente Medizin nicht möglich. Kuhn plädierte für eine Auslegung des Patientengeheimnisses, die der tatsächlichen Situation und den Patientenbedürfnissen Rechnung trage.
Magdalena Külling vom Rechtsdienst der Spitäler Schaffhausen, zeigte die Notwendigkeit zur Auslagerung aus betriebswirtschaftlicher Sicht auf. Outsourcing sei zwar unumgänglich, indessen müsse dies mit Bedacht und qualifiziert erfolgen, da damit auch ein Kontrollverlust verbunden sei.
Aus datenschutzrechtlicher Sicht hob Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich, die zusätzlichen Risiken des Outsourcing hervor, wie Verlust der Kontrolle über die Datenbearbeitung, der Nachvollziehbarkeit oder der Risiken des Datenmissbrauchs. Je grösser diese Risiken, desto höher seien die Anforderungen an die organisatorischen und technischen Massnahmen.
In der anschliessenden Podiumsdiskussion mit Vertreterinnen und Vertretern aus Patientenorganisationen, des Gesundheitsrechts, der Ärzteschaft sowie des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten wurde die Wichtigkeit der Aufklärung des Patienten betont, auch im Hinblick auf die Einführung des elektronischen Patientendossiers. Gesetzliche Anpassungen seien wohl unumgänglich, insbesondere um einen Mindeststandard für ein Outsourcing festzulegen.

### Lösungsvorschlag von privatim

privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, setzt sich für einen starken Schutz der Gesundheitsdaten ein. Der Trend zur Auslagerung lässt sich allerdings nicht aufhalten. Als pragmatische Lösung schlägt privatim eine Mittellösung vor: Die Auslagerung müsse das Patientengeheimnis wahren, d.h. der externe Dienstleister darf keine Kenntnis der Gesundheitsdaten erhalten. Konkret dürfen Gesundheitsdaten nur verschlüsselt ausgelagert werden und der Schlüssel müsse beim Spital oder Arzt verbleiben.

## Social Media und Datenschutz unter dem menschenrechtlichen Aspekt

—

*Das Schweizerische Kompetenzzentrum für Menschenrechte organisierte in Zürich eine öffentliche Veranstaltung zum Urteil des Europäischen Gerichtshofs (EuGH) vom 6. Oktober 2015 im Rechtsstreit zwischen Maximilian Schrems und der Europäischen Kommission für Datenschutz. In diesem Urteil geht es um die Rechtmässigkeit der Weiterleitung von Daten der Nutzer des sozialen Netzwerks Facebook in die USA. Maximilian Schrems vertritt die Ansicht, die Weitergabe seiner Daten durch Facebook an den US-Geheimdienst NSA sei der Beweis dafür, dass die Daten nicht geschützt sind. Können wir Facebook, Twitter und Co nutzen, ohne dass unsere Privatsphäre verletzt wird?*

Entsprechend den in den europäischen Datenschutzrichtlinien aufgestellten Regeln ist die Übermittlung von personenbezogenen Daten in einen Drittstaat an die Bedingung geknüpft, dass dieser Staat ein angemessenes Schutzniveau für diese Daten bietet. Ursprünglich befand die EU-Kommission, die USA böten einen adäquaten Schutz. Der Gerichtshof hat diesen Entscheid für ungültig erklärt und kommt zum Schluss, dass es Aufgabe der irischen Datenschutzbehörden bleibt, die Sicherheit des Drittstaats punkto Datenschutz einzuschätzen. Diese Behörden müssten anschliessend den Fall an den Gerichtshof weiterleiten, da dieser gegebenenfalls allein die Möglichkeit hat, einen Kommissionsentscheid für ungültig zu erklären. In diesem Fall erfüllen die USA die Anforderungen an einen angemessenen Schutz nicht, anders als von der Kommission festgestellt worden war (Urteil vom 6. Oktober 2015, Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650).
Im Anschluss an dieses Urteil wurde das Datenschutzabkommen «Safe Harbor» aufgehoben, das die Datenübermittlung zwischen der EU und den USA regelte. Das Abkommen wurde durch eine neue Vereinbarung namens «Privacy Shield» ersetzt.

### Auswirkungen des Entscheids

Die neue Vereinbarung enthält insbesondere die Möglichkeit des «Opt-out », das heisst, dass die betroffene Person entscheiden kann, ob ihre Daten zu einem anderen als dem ursprünglich vertraglich vereinbarten Zweck an Dritte weitergegeben werden dürfen. Mit Bedauern wurde festgestellt, die Vereinbarungsunterzeichnenden hätten keinerlei Möglichkeit, die Datenbearbeitung selber zu regeln (insbesondere das Beschaffen oder das Speichern). Sich an Unternehmen zu wenden, die personenbezogene Daten verwalten, löst das Problem nicht. Das Urteil des EuGH wirkt sich hauptsächlich auf Facebook aus und kann nicht unbedingt für alle Unternehmen zur Anwendung kommen. Strategisch gesehen ist das Verhalten einer Firma, deren Geschäftszweck im Beschaffen von Personendaten zu kommerzieller Verwendung besteht, vorhersehbar. Leider gibt es andere Unternehmen, denen mit den geltenden Datenschutzvorschriften nicht beizukommen ist, auch nicht mit «Privacy Shield». Es sind dies Organismen, die versuchen, über die Grenzen hinauszugehen, die mit der Datenbearbeitung erreicht werden können: «Wie weit können wir gehen?». Diese Debatte ist in wirtschaftlicher Hinsicht problematisch, aber einige Diskussionsteilnehmer sahen auch einen politischen Aspekt. Heute ist allgemein bekannt, dass die in den USA angesiedelte NSA Benutzerdaten bearbeitet. Heikler ist die Frage, ob Daten in andere Länder wie China oder Russland gelangen und dort bearbeitet werden, denn dann geht die Kontrolle über die Daten verloren. Hier stösst das «Privacy Shield»-Abkommen an seine Grenzen, da es nur für Daten gilt, die in die USA übermittelt werden.
Folglich ist selbst mit den gegenwärtigen Instrumenten auf Schweizer und europäischer Ebene ein absoluter Schutz der Daten, wie man ihn sich wünschen könnte, schwer zu erreichen. Grund dafür sind hauptsächlich die fehlenden Mittel.

## Moneyhouse AG muss ihre bisherige Datenbearbeitungspraxis anpassen

—

Das Bundesverwaltungsgericht heisst die Klage des Eidg. Datenschutzbeauftragten gegen die seitens der Moneyhouse AG praktizierte Datenbearbeitung grösstenteils gut. Es stellt insbesondere fest, dass auf www.moneyhouse.ch Persönlichkeitsprofile erstellt oder bearbeitet werden, sofern Angaben über Leumund, Familienverhältnisse, Ausbildung und berufliche Tätigkeit sowie Wohnverhältnisse bekannt gegeben werden. Die Moneyhouse AG wird folglich angewiesen, für solche Datenbekanntgaben die ausdrückliche Einwilligung der betroffenen Personen einzuholen. Dieses Urteil kann beim Bundesgericht angefochten werden.

*(Medienmitteilung des Bundesverwaltungsgerichts vom 11. Mai 2017; Urteil A-4232/2015 vom 18. April 2017).*

# Informationen an öffentliche Organe

## Angepasste Verordnung über den Zugang zu Dokumenten in Vernehmlassung

Seit Mitte Juni ist der Verordnungsentwurf zur Änderung der Verordnung über den Zugang zu Dokumenten (DZV) in der Vernehmlassung. Die Änderung der DZV ist eine Folge der im letzten Jahr verabschiedeten Anpassung des Gesetzes über die Information und den Zugang zu Dokumenten (InfoG) an die Aarhus-Konvention. Gewisse Anpassungen sind nötig, weil einerseits die vom Gesetzgeber gemachten Änderungen beim InfoG sich nicht auf den Umweltbereich beschränken, und andererseits die Verfahrensordnung geändert hat und auf Verordnungsebene festgelegt werden muss. Der Entwurf beantragt ausserdem einige Anpassungen der Verordnung, welche die Erfahrungen der ersten 6 Jahre bei der Anwendung der Gesetzgebung über den Zugang zu Dokumenten berücksichtigen. Die Vernehmlassung läuft bis Ende August.

## Zugang zu Dokumenten bezüglich privater Informanten der Polizei

Die Transparenzbeauftragte hat sich in einer Empfehlung dafür ausgesprochen, dass die Kantonspolizei teilweise Zugang zu einem Dokument gewähren soll, aus dem ersichtlich wird, wie das Verhältnis zwischen der Freiburger Kantonspolizei und ihren privaten Informanten sowie deren Entgeltung geregelt ist. Zum jährlichen Budget der Kantonspolizei zur Entgeltung ihrer privaten Informanten empfahl die Transparenzbeauftragte vollständigen Zugang zu geben. Ein Journalist hatte entsprechenden Zugang verlangt und dieser war mit der Begründung abgelehnt worden, dass der Einblick in die verlangten Dokumente die öffentliche Sicherheit verletzen würde. Die genannte Ausnahmebestimmung des InfoG rechtfertigte allerdings in den Augen der Transparenzbeauftragten im konkreten Fall keine vollständige Ablehnung des Zugangsgesuchs. Sie wies in ihrer Empfehlung vielmehr darauf hin, dass die Kantonspolizei jene Stellen, die unter die Ausnahmebestimmung fallen, einschwärzen solle.

**Kantonale Behörde für Öffentlichkeit und Datenschutz** ÖDSB
Chorherrengasse 2, CH-1700 Freiburg
T. +41 26 322 50 08, secretariatatprd@fr.ch
-
www.fr.ch/atprd
-
Juni 2017