Newsletter
#02 / 2014

—

Liebe Leserin, lieber Leser,

Datenschutz und Archive haben durchaus Gemeinsamkeiten, wie kürzlich die Studientage zum Thema Gerichtsarchive gezeigt haben. Dies trifft auch auf Gerichtsarchive zu. Beiden ist der sorgsame Umgang mit Daten ein Anliegen. Während beim Datenschutz die Persönlichkeitsrechte des Einzelnen im Vordergrund stehen und Schutzobjekt sind, dienen Archive als Gedächtnis der Gesellschaft. Für den Datenschutz folgt aus dem Verhältnismässigkeitsprinzip, dass Personendaten zu vernichten oder zu anonymisieren sind, wenn sie nicht mehr benötigt werden; dies allerdings unter dem Vorbehalt der Bestimmungen über die Archivierung. Demgegenüber beschäftigt sich die Archivierung mit dem zeitgeschichtlichen Aspekt. Hier geht es um den Schutz von Daten und Materialien im Hinblick auf die Erhaltung von Zeitdokumenten.
Werden Personendaten archiviert, ändert sich der Zweck ihrer Erhebung: Geht der Datenschutz von der zweckgerichteten Datenbearbeitung und der Vernichtung der Daten aus, wenn diese nicht mehr gebraucht werden, steht bei der Archivierung die Aufbewahrung und Konservierung der Daten zur Dokumentation der Zeitgeschichte im Vordergrund. Der bewusste und sorgsame Umgang mit Personendaten zeigt sich indessen darin, dass archivierte Daten und Informationen nicht unmittelbar mit ihrer Archivierung der Öffentlichkeit zugänglich werden, sondern erst nach Ablauf einer Schutzfrist. Für Dokumente mit Personendaten, mithin auch sensiblen Personendaten, wie sie polizeiliche Dokumente und Gerichtsakten beinhalten, sind angemessene Schutzfristen vorzusehen. Die Gesetzgebung des Kantons Freiburg bezeugt insoweit einen bewussten Umgang mit Personendaten und zeigt auf, dass Persönlichkeitsrechte ernst genommen werden. Es ist zu begrüssen, dass der Vorentwurf zu einem kantonalen Archivgesetz ausgedehnte Schutzfristen vorsieht. Dies ist in der heutigen Zeit mit den unzähligen Informationsquellen, Publikationsmedien, sozialen Medien und namentlich dem Internet, das kein «Recht auf Vergessen» kennt, überaus wichtig. Die neuen Medien lassen auch nach Jahren die «Lebensgeschichte» einer Person nachvollziehen. Eine vorzeitige Öffnung von Gerichtsarchiven lässt die Persönlichkeitsrechte betroffener Personen und deren Familie nicht unberührt. Im Gegenteil: Archivierung ohne hinreichende Schutzfristen kann – in Verbindung mit neuen Medien – Persönlichkeitsverletzungen perpetuieren. Vor diesem Hintergrund und insbesondere unter Berücksichtigung des Rechts auf Vergessen zeigt der Vorentwurf mit seinen vorbildlichen Schutzfristen den richtigen Weg auf.

Alice Reichmuth Pfammatter
Kantonale Datenschutzbeauftragte

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

Siebter Schweizerischer Datenschutzrechtstag

Der diesjährige Schweizerische Datenschutzrechtstag an der Universität Freiburg setzte den Schwerpunkt auf die «Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes». Die immer rasantere technologische Entwicklung hat zum Aufkommen neuer Datenschutzinstrumente wie Privacy by Design, Recht auf numerisches Vergessen und auch unternehmensinterne Datenschutzregelungen geführt.

Die aktuellen Herausforderungen mit dem technischen Fortschritt und geänderten Verhaltensweisen veranlassen die verschiedenen zuständigen Organe zu reagieren. Im März 2014 verabschiedete das Europäische Parlament Änderungen am Entwurf einer allgemeinen Datenschutzverordnung, so die Stärkung der Rechte der betroffenen Personen sowie die Einführung neuer Datenschutzinstrumente wie Privacy by Design.

Datentransfer

Heute sind neue Instrumente wie die BCR (Binding corporate rules oder verbindliche unternehmensinterne Datenschutzregelungen) zu berücksichtigen. Es handelt sich um Compliance-Instrumente, mit denen sich die Datentransfers in internationalen Konzernen regeln lassen, wie Myriam Gufflet erklärte, die Verantwortliche des BCR-Zentrums, Compliance-Abteilung bei der Commission nationale française de l'informatique et des libertés (CNIL), der französischen Datenschutzbehörde. Obschon die Schweiz noch nicht direkt betroffen ist, scheint mit Blick auf die Multis wie Nestlé, ADM, Adecco u.a. eine kurze Einführung angebracht.
Die BCR zielen auf Datentransfers ausserhalb des Europäischen Wirtschaftsraums (EWR) ab. Grundsätzlich sind Datentransfers verboten (Art. 25 der EU-Datenschutzrichtlinie 95/46/EG), von Ausnahmen abgesehen. So muss das Land oder das Unternehmen, das von dieser Möglichkeit Gebrauch machen möchte (Datentransfer ausserhalb EWR), ein angemessenes Datenschutzniveau bieten und auch weitere Auflagen einhalten, wie die Vornahme durch Mustervertrag geregelter Datentransfers. Ob das Datenschutzniveau ausreichend ist, wird von der Europäischen Gemeinschaft (EG) beurteilt. Myriam Gufflet führte in ihrem Referat aus, dass die BCR ein Verhaltenskodex sind, der die

globale Unternehmenspolitik in Bezug auf den Transfer personenbezogener Daten ausserhalb des EWR definiert. Daher werden mit der Einführung von BCR im Unternehmen die Datenverwaltung und der Datentransfer innerhalb des Konzerns einfacher.

Durchsetzung der Datenschutzrechte

Das Zitat des Tages: «Ich weiss, dass ich nicht weiss…» illustriert die aktuelle Situation sehr gut. Olivier Gnehm, Rechtsanwalt in Zürich, wählte als Einstieg in seinen Vortrag dieses Zitat von Plato mit dem Nachtrag « …ob und wie meine Personendaten bearbeitet werden». Wie Jean-Philippe Walter, Stellvertreter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, ausführte, sind nicht nur die Privatpersonen in Unkenntnis ihrer Rechte, sondern kennen auch die Verantwortlichen für die Datenbearbeitung das Bundesgesetz über den Datenschutz (DSG; SR 235.1) und die geltenden Datenschutzinstrumente zu wenig. Dies kommt hauptsächlich darin zum Ausdruck, dass die von den Bundesbehörden gebotenen Möglichkeiten zu wenig genutzt werden. Monique Cossali Sauvain, Chefin des Fachbereichs Rechtsetzungsprojekte und -methodik beim Bundesamt für Justiz (BJ) bestätigte, dass die Überlegungen im Hinblick auf eine Revision des Gesetzes (DSG) namentlich dahin gehen, die betroffenen Personen besser zu sensibilisieren, wobei zusätzlich aber auch ein optimaler Schutz angestrebt werde, um allfällige Probleme schon in der Konzipierungsphase neuer Technologien zu erkennen.

Digitale Identität

Nach den Worten von Stéphane Koch, Vize-Präsident der High-Tech Bridge AG, besteht unsere Identität aus Facetten, die je nach sozialem Kontext unterschiedliche Ausdrucksformen annehmen. In der heutigen modernen Zeit die Kontrolle über die eigene digitale Identität zu behalten, sei manchmal eine Herausforderung, und obschon die meisten sozialen Netzwerke oder anderen Plattformen (wie Facebook, Twitter, LinkedIn, Instagram, Skype usw.) verschiedene Möglichkeiten vorsehen, unsere Daten zu sichern oder sogar zu löschen, sei dies nicht immer ausreichend. So ist es ganz entscheidend, das «Recht auf Vergessen», die Notwendigkeit der digitalen Existenz, die Meinungsfreiheit und das Recht auf Information miteinander in Einklang zu bringen. Und auch wenn die betroffenen Personen heute unbestrittenermassen nach Ablauf einer gewissen Zeit grundsätzlich das Recht haben, sich der Veröffentlichung von der Vergangenheit angehörenden Tatsachen zu widersetzen (Recht auf Vergessen), so ist doch eine Abwägung der bestehenden Interessen wesentlich. Die Medien hätten beispielsweise keine Hemmungen, aus jeder noch so unbedeutenden Information so viel wie möglich herauszuholen; wir könnten uns mit dem Recht auf Vergessen dagegen wehren.
Ein erster Sieg ist mit dem Urteil des Europäischen Gerichtshofs errungen worden, wonach alle natürlichen Personen das Recht haben zu verlangen, dass Suchmaschinen die sie betreffenden personenbezogenen Informationen in den Suchresultaten löschen.
Bemerkenswert: Als Google mit der Bereitstellung eines Formulars zur Geltendmachung des «Rechts auf Vergessen» reagierte, gingen innerhalb von 24 Stunden 12 000 Löschanträge ein. Stéphane Koch ist gespannt, wie Google mit diesem neuen Instrument weiter verfahren wird.

Unterschiedliche Fragestellungen

Der letzte Redner des Tages, Prof. Alexandre Flückiger, Vizedekan und Professor an der Universität Genf, gab einen kurzen Überblick über die jüngsten Bundesgerichtsentscheide mit Bezug zum Datenschutz. Er legte dar, wie unterschiedlich die Fragen sind, die sich diesbezüglich stellen (von der Unabhängigkeit einer Datenschutzkontrollbehörde über Personenkontrollen an Sportanlässen oder die Berichtigung von Protokollen bis zur Verwaltung von Spitaldossiers). Alle diese Urteile zeigen, dass der Datenschutz in unserer Gesellschaft wichtig ist und eine nicht unwesentliche Rolle spielt.

Dieser siebte Datenschutzrechtstag unter der Leitung von Professorin Astrid Epiney von der Universität Freiburg ging mit einer klaren Feststellung zu Ende: Die Schweiz kann nicht ohne Rücksicht auf ihre Nachbarn handeln. Aufgrund der Schengen- und Dublin Abkommen muss die Schweiz europarechtskonform sein; interessantes Vorbild und mögliche Referenz für eine effiziente und pragmatische Revision. Demzufolge sind die Notwendigkeit, Massnahmen in Bezug auf die Vollzugsmechanismen zu treffen, angemessene Datenschutzinstrumente einzuführen sowie unsere Gesetze der gesellschaftlichen Realität anzupassen, die Zukunftsaussichten für das Datenschutzrecht.

Symposium on Privacy and Security

—

Ende August fand in Zürich das 19. Symposium on Privacy and Security statt, eine dem Datenschutz und der Informatiksicherheit gewidmete Tagung mit dem Titel «Datenschutz in der Datenflut? «Big Data Analytics» – Möglichkeiten und Herausforderungen. Technische, rechtliche und gesellschaftliche Konzepte auf dem Prüfstand».

In unserer digitalen Welt erscheint die Sicherheit als immer fragiler, die Informationstechnologie zeigt sich als eigentliche Risikotechnologie, die Grundwerte der Gesellschaft wie persönliche Freiheit und Sicherheit in Frage stellt. Da das Datenschutzkonzept kaum mehr greift und Reformen stocken, scheint die Sensibilisierung der Bevölkerung auf den Selbstschutz (sachgemässe Internetnutzung, IT-Kenntnis und -Verständnis usw.) die schnellste Lösung zu sein, wenn Rechts- und Sicherheitsinfrastrukturen fehlen.

Big Data

Datenvolumen und –verfügbarkeit sind rapid angewachsen und führen für die Wirtschaftssektoren zu einer Annäherung zwischen «Big Data» und «Big Business». Anders gesagt sind diese von unserer Informationsgesellschaft generierten und entwickelten Daten neue ökonomische Werte auf dem Markt (z.B. Amazon, Zalando, Facebook, Whatsapp usw.). Prof. Thomas Hofmann, Professor für Data Analytics am Departement Informatik an der ETH Zürich, hat diese Informationsmasse unter drei Gesichtspunkten präsentiert: «Volume», «Velocity» und «Variety». «Volume» bedeutet, dass das Anwachsen der globalen Datenbestände nicht nur auf das World Wide Web und die «Smart Devices» wie Smartphones und Tablets zurückzuführen ist, sondern auch auf die Nutzung durch den Menschen. Professor Hofmann drückt dies so aus: alle Informationen auf Google, alle Menschen auf Facebook und alle Waren auf Amazon.

Gesteigert wird diese Informationsflut noch durch die Art ihrer Erzeugung. Heute wird eine grosse Datenmenge durch ein System automatischer Selbsterzeugung generiert (Sensoring, Tracking, Umwelt, Self-Posting usw.). Diese Eigenproduktivität ist das, was Professor Hofmann «Velocity» nennt. Ausserdem wird diese «Velocity» durch ihre Diversität charakterisiert. So hat diese selbsterzeugte Datendichte unterschiedliche Quellen (Websurfing, Kassentickets, soziale Netze, Geolokalisierung usw.), besteht aber auch aus unterschiedlichen Datentypen an sich (Personalien, Bankauszüge, soziale Daten usw.). Daher führt «Big Data» nicht nur zu Änderungen in verschiedenen Industriezweigen mit einem wirtschaftlichen Potenzial für uns (Medien, Werbung, E-Commerce, Gesundheit, Erziehung usw.), sondern durch das Wegfallen von Grenzen auch zu einem Kontrollverlust und wird zu einer Gefahr für den Datenschutz, insbesondere durch politischen Missbrauch und Regierungsinteressen – man denke nur an den Fall von Edward Snowden.

IT – Angemessener Schutz?

Heute hat der Normalbürger mit den neuen Kommunikationstechnologien und –mitteln einen angemessenen Schutz seiner Daten mehr als nötig. An dieser Tagung sprach Professor Norbert Pohlmann vom Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule über die vier grossen Herausforderungen für die Informatiksicherheit: Sensibilisierung gegenüber den schützenswerten Daten, Vorbeugen vor Angriffen, Erkennen von Angriffen und Reaktion auf diese Angriffe (Gegenangriff). Überraschenderweise sind offenbar nur gerade 5% aller vorhandenen Daten in Unternehmen wirklich besonders schützenswert. Die Frage bleibt jedoch, welche Daten es sind und wie sie richtig geschützt werden können. In Bezug auf die Prävention und Sensibilisierung gilt generell das Prinzip der digitalen Sparsamkeit, das heisst so wenige Daten generieren wie möglich, so viele wie nötig. Ausserdem lassen sich mit Gegenmassnahmen der Nutzer mit der Einrichtung von Schutzsystemen (Verschlüsselungssicherheitssysteme, Authentifizierungsverfahren, vertrauenswürdige IT-Systeme, Antivirus, Antispam, regelmässiges Löschen von Caches und Cookies usw.) Risiken minimieren oder sogar ganz beseitigen (Viren, Malware, Spam usw.). Die Erfahrung hat jedoch gezeigt, dass die neuen Sicherheitstechnologien keine wirklich wirksame und verlässliche Lösung oder Software bieten. So ist die Möglichkeit gewisser Programme, alle Hackerangriffe oder Systemanomalien zu erkennen, nützlich, hat aber auch seine Grenzen.

Fakt ist, dass zwar die IT-Sicherheit grosse Lücken aufweist, die Bürger ständig Bedrohungen ausgesetzt

sind und unsere Grundwerte in gewisser Weise in Frage gestellt werden, dass aber der technische Fortschritt der heutigen Gesellschaft das Leben leichter macht und ihr eine Öffnung ermöglicht. Und gerade weil die Datenflut nicht weniger und der Informationszugang immer einfacher wird, müssen Prävention und Information der Nutzer verstärkt werden. Das Symposium wollte mit einem Überblick über die Gesamtsituation Lösungsansätze liefern und Denkanstösse geben.

IT – Fall des «Phishing»

Die IT-Sicherheit wird tagtäglich ernsthaft auf die Probe gestellt (Hacking, Identitätsdiebstahl usw.). Ein neues Phänomen für die Internetnutzer ist das «Phishing», mit dem Betrüger versuchen, an vertrauliche Daten ahnungsloser Internetnutzer zu gelangen. Das Wort Phishing setzt sich aus den englischen Wörtern «Password», «Harvesting» und «Fishing» zusammen, bildlich das Angeln nach Passwörtern. Und so funktioniert es: Über Internet oder E-Mail wird versucht, sensible Daten, Passwörter (Login), Bankdaten, E-Banking-Zugangsdaten, Informationen über Ihre Konten in Onlineshops und sogar Zugangsdaten zu E-Mail-Konten oder sozialen Netzwerken abzugreifen. Mit täuschend echten E-Mails, Links und Webseiten beabsichtigen Kriminelle, Ihnen die Zugangsinformationen zu Bankkonten oder Kreditkartendaten zu entlocken. Diese Links führen zu Websites mit Internetadressen, die denen echter Dienstanbieter ähneln (E-Banking, Onlineshops usw.). Solche Phishing-Mails können auch angehängte Dateien enthalten; wenn Sie diese anklicken, installieren Sie einen Virus, der alles registriert, was Sie in den Computer eingeben. Diese Informationen können dann von den Hackern zu missbräuchlichen Zwecken verwendet werden. Empfohlen wird, nie einen Computer gleichzeitig zu privaten und beruflichen Zwecken zu nutzen. Nutzen Sie den Computer, auf dem Sie im Netz surfen, nicht für Ihr E-Banking. Zudem sind Sicherheitszertifikate wie «https» eine Sicherheitsgarantie, auf die sich die Internetnutzer verlassen können; oft erscheint übrigens unten an solchen Seiten ein kleines Vorhängeschlosssymbol.

Transparenz – Ideologie eines politischen Leitbegriffs

In der heutigen Welt sind wir mit einer zunehmenden Masse und Verfügbarkeit unterschiedlichster Informationen konfrontiert. Unter diesem Blickwinkel sprach Prof. Manfred Schneider von der Ruhr-Universität-Bochum am 19. Symposium on Privacy and Security über die Tragweite des Transparenzprinzips als Leitbegriff für die Wirtschaft und unser tägliches Leben. Dieser Ansatz scheint einen immer grösseren Stellenwert einzunehmen. Tatsachlich beschäftigt das Streben nach Transparenz in politischer, wirtschaftlicher oder sozialer Hinsicht die Gemüter unaufhörlich. Seiner Zeit voraus, plädierte schon Jean-Paul Sartre für Transparenz («Ich denke, dass Transparenz allenthalben an die Stelle dessen treten soll, was geheim ist») und nahm den diesbezüglichen Trend vorweg, der in vielen Ländern eingesetzt hat (Aufhebung des Bankgeheimnisses im Steuerwesen oder auch der «Fall Snowden»). US-Präsident Barack Obama würdigte in seiner Antrittsrede 2009 die Bedeutung einer transparenten Politik für ein effizientes System.

Die «Transparenz» unserer Gesellschaft ist auch von ihrer urbanen Architektur geprägt. Paul Scheerbart stellt in «Glasarchitektur» neue Wege in die moderne Architektur vor (Stahlträgerkonstruktionen, Glaswände, usw.), die in seinen Augen das Leben der Menschen hätten ändern können: «Glas ist nicht umsonst ein so hartes und glattes Material, an dem sich nichts festsetzt. [...]Das Glas ist überhaupt der Feind des Geheimnisses.» So verändert die Architektur unsere Werte. Obwohl in Vergessenheit geraten, scheint sich das Projekt von Scheerbart in den grossen Metropolen und auch in einigen kleineren Städten verwirklicht zu haben. Unterwegs in diesen Stadtzentren stösst man heute überall auf grosse Gebäude mit reflektierenden Fassaden, ein Zusammenspiel von Formen und Bildern, worin wir uns bewegen. Und wie in André Bretons Roman «Nadja» lebt das Individuum scheinbar in einem Glashaus, wo dank der neuen Technologien sein ganzes Tun beobachtet und sichtbar gemacht werden kann.

Verschärfte Regeln für Drohnen

Nach den jüngsten Vorfällen mit Drohnen, wie im letzten Juni in Zürich am Konzert einer berühmten englischen Band, als eine Drohne den Zuschauern gefährlich nahe kam, hat der Bund beschlossen, die geltende Regelung zu verschärfen.

Mit dem vermehrten Aufkommen von Drohnen sah sich das Bundesamt für Zivilluftfahrt (BAZL) gezwungen zu reagieren und drängte auf eine Anpassung der Gesetzesbestimmungen. So ist die Verordnung des UVEK über Luftfahrzeuge besonderer Kategorien (VLK; SR 748.941) auf den 1. August 2014 entsprechend aktualisiert worden. Nach den geänderten Bestimmungen müssen Drohnenpiloten für den Betrieb von Drohnen im Umkreis von weniger als 100 Metern um Menschenansammlungen beim BAZL eine Bewilligung einholen.

Weiter gilt für den Betrieb von Drohnen:
- Drohnen mit einem Gewicht von bis zu 30 Kilogramm benötigen keine Bewilligung, sofern immer direkter Augenkontakt zwischen Drohnenpilot und Drohne besteht.

- Für den Einsatz von Drohnen mit einem Gewicht von mehr als 30 Kilogramm ohne direkten Augenkontakt im Umkreis von weniger als 100 Metern um Menschenansammlungen, namentlich bei «Public Viewings» und sonstigen öffentlichen Veranstaltungen, an denen mehrere Dutzend dicht beieinander stehende Personen versammelt sind, ist beim BAZL eine Bewilligung einzuholen.

Link zur Verordnung des UVEK
http://www.admin.ch/opc/de/classified-compilation/19940351/index.html

Volle Transparenz beim Einsatz öffentlicher Gelder

Auf eidgenössischer Ebene ging es im Bereich des Öffentlichkeitsprinzips im letzten Jahr häufig um den Einsatz öffentlicher Gelder. In mehreren Empfehlungen sprach sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) dabei für vollständige Transparenz aus.

Nur so könne einer Zweckentfremdung staatlicher Mittel begegnet werden, erklärte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, Hanspeter Thür, an der Jahresmedienkonferenz. Mit Sorge verfolge er deshalb die Bemühungen verschiedener Ämter und Dienststellen, sich vom Öffentlichkeitsgesetz (BGÖ) ausnehmen zu wollen. Die deswegen in Gang gesetzte Evaluation des BGÖ dürfe nicht dazu führen, dass gerade im Aufsichtsbereich, wo Transparenz sehr wichtig ist, wieder neue Dunkelkammern entstehen, die keiner Aufsicht unterworfen sind.

Dank dem steten Streben nach Transparenz seien in den vergangen Jahren auf Bundesebene einige Korruptions- und Missbrauchsfälle aufgeflogen, erinnerte Thür. So sei namentlich die Korruptionsaffäre beim Staatssekretariat für Wirtschaft nicht zuletzt dank dem BGÖ ans Licht gekommen. Dank einer Empfehlung des EDÖB seien zudem auch die Hintergründe von privaten Finanzierungen von Lehrstühlen an der ETH publik geworden, die zu einer intensiven öffentlichen Debatte führten.

In mehreren Empfehlungen waren ebenfalls die Vergabe von Subventionen und Innovationsgeldern sowie die Offenlegung von Verträgen zwischen der Bundesverwaltung und von ihr beauftragten Gutachtern und Unternehmen und die Interessenbindung von Bundesangestellten Thema. «In allen Fällen geht es um die Frage, wie öffentliche Gelder eingesetzt werden. Wir sind klar der Meinung, dass in all diesen Fällen vollständige Transparenz hergestellt werden muss», so Thür.

Informationen an öffentliche Organe

Schlichtungsantrag zu Dokumenten der PUK Poya

Bei der Öffentlichkeitsbeauftragten ging ein Schlichtungsantrag von einer Journalistin ein, die bei der Parlamentarischen Untersuchungskommission PUK Poya Zugang zu sieben Interviews mit politischen Entscheidungsträgern und Projektbeteiligten verlangt hatte, die von der PUK Poya durchgeführt, aber nicht zusammen mit dem Schlussbericht veröffentlicht worden waren. Die PUK Poya lehnte den Zugang zu den Dokumenten ab, da es sich dabei um Protokolle nicht öffentlicher Sitzungen handle, die laut InfoG nicht zugänglich seien.
Die Öffentlichkeitsbeauftragte nahm daraufhin Einblick in die gewünschten Dokumente und kam ebenfalls zum Schluss, dass es sich dabei um Protokolle nicht öffentlicher Sitzungen handelt. Sie wies das Sekretariat des Grossen Rates aber darauf hin, dass für die in Art. 29 InfoG genannten Fälle zwar keine Zugangsgarantie bestehe, das öffentliche Organ aber durchaus freiwillig Zugang gewähren könne, sofern alle Beteiligten einverstanden seien. Das öffentliche Organ holte daraufhin dieses Einverständnis ein und die Dokumente konnten der Journalistin zugestellt werden.

Leitfaden zum Zugangsrecht für öffentliche Organe aktualisiert

Der Leitfaden zum Zugangsrecht für öffentliche Organe ist nach Inkrafttreten der Aarhus-Konvention für die Schweiz aktualisiert worden und auf unserer Website verfügbar. Werfen Sie einen Blick hinein! (http://www.fr.ch/atprd/de/pub/publikationen/oeffentlichkeit/guide_pratique.htm)

Experten- und Studiendatenbank zum Öffentlichkeitsprinzip

Auf der Internetplattform www.oeffentlichkeitsgesetz.ch befindet sich neu eine Experten- und Studiendatenbank zum Öffentlichkeitsprinzip. Mehr als 120 Studien und wissenschaftliche Aufsätze rund ums Öffentlichkeitsprinzip in den Verwaltungen von Bund, Kantonen und anderen Ländern wurden darin zusammengetragen. Sie stammen von über 50 Expertinnen und Experten, die mit ihren Werken und den Koordinaten abrufbar sind.

Installation einer Webcam

Eine Gemeinde hat mit unserer Behörde Kontakt aufgenommen, um Details des Vorgehens bei der Installation einer Videoüberwachungskamera im Falle einer Privatperson zu erfahren, deren Kamera ganz oder teilweise öffentlichen Grund erfasst. Laut Art. 1 Abs. 3 des Gesetzes vom 7. Dezember 2010 über die Videoüberwachung (VidG) versteht man unter Videoüberwachung jede mit technischen Hilfsmitteln durchgeführte Beobachtung von Personen oder Sachen mit dem Ziel der Überwachung. Die Botschaft des Staatsrats vom 6. Juli 2010 zum Vorentwurf des Gesetzes über die Videoüberwachung erwähnt ausdrücklich, dass das Gesetz lediglich die Installationen abdeckt, die zur Beobachtung von Personen zur Überwachung (abschreckende Videoüberwachung) dienen und nicht diejenigen, welche einen touristischen Zweck verfolgen. Letztere benötigen keine Bewilligung, sie müssen aber die Regeln des Datenschutzes befolgen. Aus dem VidG und der Botschaft geht also klar hervor, dass der Zweck der Installation entscheidend dafür ist, ob das VidG für die Installation einer Webcam massgebend ist. Wenn mit der Kamera ein touristischer Zweck verfolgt wird, fällt deren Installation nicht unter das VidG, es müssen aber die Regeln des Datenschutzes befolgt werden. Wird die Webcam hingegen zum Zweck der Überwachung installiert, ist das VidG massgebend und eine Bewilligung durch die Oberamtsperson des betroffenen Bezirks ist notwendig.

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
-
Dezember 2014