Newsletter
#02 / 2017

Liebe Leserin, lieber Leser
Wie alle öffentlichen Organe steht auch unsere Behörde in ihren Tätigkeitsbereichen vor einem ständigen Wandel und stets neuen Herausforderungen. Dabei ist es uns ein Anliegen, dass die betreffenden gesetzlichen Grundlagen diesem Wandel Rechnung tragen. Im Bereich Transparenz ist eine entsprechende Aktualisierung nun gerade zu Ende gegangen und schon hat parallel die Aktualisierung des Datenschutzgesetzes begonnen. In beiden Fällen geht es unter anderem darum, unsere kantonalen Rechtsgrundlagen mit internationalen Regelwerken in Einklang zu bringen.

So wurde das Gesetz über die Information und den Zugang zu Dokumenten (InfoG) im letzten Jahr an die Aarhus-Konvention angepasst, die für die Schweiz im Umweltbereich bindend ist. Auf 1. Januar 2018 tritt nun die angepasste Verordnung über den Zugang zu Dokumenten (DZV) in Kraft. Sowohl beim Gesetz als auch bei der Verordnung wurden neben den unabdinglichen Änderungen auch einige Anpassungen angebracht, welche die Erfahrungen der letzten 7 Jahre bei der Anwendung der Gesetzgebung über den Zugang zu Dokumenten berücksichtigen.

Im Datenschutz stehen ebenfalls bedeutsame Änderungen der Gesetzgebung an. Der Bundesrat hat am 15. September 2017 den Vorentwurf sowie die Botschaft zur Totalrevision des eidgenössischen Datenschutzgesetzes veröffentlicht. Dieser soll der Revision der EU-Datenschutzgesetzgebung Rechnung tragen, damit die Schweiz weiterhin über ein angemessenes Datenschutzniveau verfügt. Dies ist vor allem für die Wirtschaft wichtig, damit der Datenaustausch mit der EU nicht übermässig erschwert wird.

Aber auch auf kantonaler Ebene ist zu prüfen, ob und inwieweit das kantonale Datenschutzgesetz anzupassen ist. Hier gilt es insbesondere die modernisierte Europaratskonvention SEV 108 sowie die EU-Richtlinie 2016/680 miteinzubeziehen. Letztere ist Teil des Schengen-Acquis. Wollen die schweizerischen Behörden, insbesondere im Polizei- und Strafrechtsbereich weiterhin über Zugriff zum Schengener Informationssystem SIS verfügen, ist auch die kantonale Gesetzgebung zu revidieren.

Neben diesen gesetzlichen Anpassungen gibt es auch viele andere aktuelle Themen in unseren Tätigkeitsbereichen, wovon einige im vorliegenden Newsletter aufgegriffen werden. Wir wünschen Ihnen eine angenehme Lektüre!

Alice Reichmuth Pfammatter
Kantonale Datenschutzbeauftragte

Annette Zunzer Raemy
Kantonale Beauftragte für Öffentlichkeit und Transparenz

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

Weiterentwicklung von Open Data in der Schweiz

An der diesjährigen Jahrestagung von Opendata.ch ging es um die Zukunft der Offenen Daten in der Schweiz. Ob in der Wissenschaft oder in der Nahrungsmittelbranche, ob in der Stadtentwicklung, im Tourismus oder im Transportwesen: Offene Daten und Dateninfrastrukturen werden heute in ziemlich allen Lebensbereichen von fast jedem genutzt.

Vertreterinnen und Vertreter der digitalen Gesellschaft gaben an der Tagung Einsichten in diese Bereiche und diskutierten mit den Teilnehmenden aus Verwaltung, Wirtschaft, Wissenschaft, Politik, Journalismus und IT Entwicklungskonzepte, die darauf abzielen, mit Hilfe von Offenen Daten mehr Effizienz, Transparenz und Innovation sowie ein ökologisch, technologisch und sozial fortschrittliches Umfeld zu gestalten.

Stärken der Schweiz

So plädierte Peter Delfosse, CEO des in der Digitalisierung aktiven Unternehmens Axon Active, dafür die Daten auf Langfristigkeit auszulegen und in Ökosystemen zusammenzubringen. Daten seien kein Verbrauchsgut, sondern ein Investitionsgut, sagte Delfosse. Die Stärken der Schweiz in diesem Prozess seien die Rahmenbedingungen und die Innovationskraft, die es zu nutzen gelte. Entscheidend seien zudem das Bekenntnis zu Open Data auf der obersten Führungsebene, die Befähigung der Verwaltung zur digitalen Transformation und der Einbezug von Bevölkerung und Parlamenten.

Simon Hodson, Geschäftsführer von CODATA, dem Committee on Data for Science and Technology, wies darauf hin, dass dringend in Dateninfrastruktur investiert werden müsse – so wie in früheren Zeiten in Bibliotheken investiert worden sei. Zudem sei es im wissenschaftlichen Bereich unerlässlich, dass parallel zu wissenschaftlichen Studien die zugrundeliegenden Daten veröffentlicht werden. Ansonsten sei Wissenschaft nicht transparent.

Rahel Ryf von der Open-Data-Plattform öV Schweiz zeigte an der Tagung auf, wie die digitale Zukunft des öffentlichen Verkehrs mit Open Data gestaltet werden kann und Pascal Jenny, Tourismusdirektor aus Arosa erläuterte das Potenzial von offenen Daten für den Schweizer Bergtourismus.

Vielfältiger Nutzen

Andreas Kellerhals, Direktor des Schweizerischen Bundesarchivs, seinerseits gab einen Überblick über den aktuellen Stand und die Aus- und Absichten von opendata.swiss, dem Portal der Schweizer Behörden für frei verfügbare Daten. Im Vergleich zum letzten Jahr sei ein Zuwachs an Daten von fast 90% zu verzeichnen und entsprechend habe auch die Datennutzung auf dem Portal zugenommen, erklärte Kellerhals. Da die derzeitige Strategie im kommenden Jahr ablaufe, gelte es nun diejenige ab 2019 zu definieren.

Ein Blick in die über 30 aus Daten von opendata.swiss entstandenen Anwendungen zeigt, wie vielfältig deren Nutzen sein kann: So können die Berge in den Schweizer Alpen und der Ursprung ihrer Namen erkundet werden und in einer partizipativen Zeitmaschine kann man durch Landschaften, welche in der Vergangenheit fotografiert wurden, navigieren. Ein Reiseassistent kann Fragen zum Fahrplan in einer einfachen Konversation beantworten und andere Apps wiederum erlauben in der Stadt Zürich das am nächsten gelegene, öffentliche WC schnell zu lokalisieren und aufzusuchen sowie freie Parkhausplätze oder Verfügbarkeiten von Leihfahrrädern in Echtzeit zu konsultieren.

Cookies und Tracking

«Wollen Sie Cookies zulassen?» Diese Frage begegnet uns laufend beim Besuch von Internetseiten. Wie funktionieren diese?
Cookies sind Dateien, die beim Besuch von Websites durch den Browser auf dem verwendeten Computer abgespeichert werden (Steiger Martin, Rechtskonforme Cookies auf Websites nach europäischem und schweizerischem Recht, in Anwaltsrevue 2015, S. 18-21). Sie sind wie eine Visitenkarte jedes einzelnen Besuchers einer Website. So wird man bei einem erneuten Besuch der Website als Nutzerin oder Nutzer wiedererkannt und in gewissem Masse auch über das Verhalten auf der Website, etwa über den Benutzernamen, die besuchten Seiten, die Anzahl Klicks oder die Scrolls.
Cookies hinterlassen Spuren. Sind diese mit weiteren Informationen verknüpft, so können sie ein Persönlichkeitsprofil bilden und damit Personen erkennbar werden lassen. Dies ist eine Verwendungsmöglichkeit der Webtracking-Dienste. Allerdings sind nicht alle Cookies schädlich.
Einige sind sogar nützlich, um im Internet ohne Informationsverlust von Seite zu Seite surfen zu können. Dies macht auch Online-Shopping möglich; Cookies sind nämlich erforderlich, um beispielsweise einen Warenkorb auf einer E-Commerce-Website zu pflegen. Auch die Informationen in der Mailbox werden mit Hilfe von Cookies verwaltet.
Der Entwurf der neuen sogenannten Cookie-Richtlinie der Europäischen Union (bisherige Richtlinie 2009/136/EG) sieht eine Vereinfachung der Vorschriften für die Verwendung von Cookies vor. An sich können die Nutzerinnen und Nutzer die Cookies direkt in ihren Browsereinstellungen blockieren, aber es braucht keine Einwilligung eingeholt zu werden für die Verwendung von Cookies, die für das Surfen auf Websites notwendig sind, sowie für Cookies zur Ermittlung der Besucherzahlen auf der Website. Die in der Schweiz geltende, weniger restriktive Praxis ist in den Artikeln 45c und 53 des Fernmeldegesetzes vom 30. April 1997 geregelt (SR 784.10; FMG). Demnach müssen die Nutzerinnen und Nutzer über die Verwendung von Cookies und den Grund ihrer Verwendung informiert werden. Sie können diese Bearbeitung nach dem «Opt-out-Prinzip» ablehnen.

Analyse der Praktiken von Facebook

Am zehnten Schweizerischen Datenschutzrechtstag, der in Freiburg stattfand, befasste sich ein Workshop mit der Datenbearbeitung durch die sozialen Netzwerke, wobei einige Praktiken von Facebook unter die Lupe genommen wurden.

Nach Definition der Akteure, des geltenden Rechts, der sensiblen und der nicht sensiblen Daten, des Persönlichkeitsprofils und der Datenbearbeitung wurde auf das eidgenössische Datenschutzgesetz (DSG) eingegangen, da Facebook als Privatperson gilt. Damit ein soziales Netzwerk Personendaten bearbeiten kann, braucht es Rechtfertigungsgründe. Facebook stützt sich dazu auf die Vertragsbindung mit den Nutzern, und zwar auf die Allgemeinen Nutzungsbedingungen (ANB; beispielsweise für die Kontoeinrichtung, die Verwaltung von Freunden usw.). Im Übrigen beruft sich Facebook auf die Zustimmung der Nutzer und geht grundsätzlich davon aus, dass wer ein Facebook-Profil hat, mit jeglicher Datenbearbeitung durch Facebook einverstanden ist. Aus der Analyse geht klar hervor, dass Facebook eine dominierende Stellung hat und den Nutzern wenig Spielraum bleibt. Entweder akzeptieren sie alles, oder sie verzichten auf die Nutzung von Facebook.

Beim Durchlesen der ANB fällt insbesondere auf, dass sie vage sind, dass dem Bearbeiten keine Grenzen gesetzt sind, dass die Daten für Forschungszwecke verwendet und mit anderen Apps geteilt werden. Dazu kommt, dass die Nutzer die ANB meistens gar nicht durchlesen, weil sie so komplex, technisch und sehr ausführlich sind. So erlaubt sich Facebook trotz Änderung in den Einstellungen enorme Mengen unserer Daten mit unserer «Pseudo-Zustimmung» zu bearbeiten, da die Nutzer nicht klar darüber informiert werden, was alles mit ihren Daten geschieht. Dies legt den Schluss nahe, dass in den sozialen Netzwerken ein grosser Transparenzbedarf besteht und es eine strenge und flexible Regelung braucht, vor allem aber juristische und technische Mittel, um sie zur Anwendung zu bringen und dafür zu sorgen, dass sie auf internationaler Ebene eingehalten wird. Man darf nicht vergessen, dass Facebook mit der künstlichen Intelligenz (Spracherkennung, Gesichtserkennung) immer mehr Daten sammelt und in der Lage ist, Persönlichkeitsprofile zu erstellen.

Vernetzte Autos und Datenbearbeitung

Wer im Auto das Navi einschaltet oder Musik hört, muss sich bewusst sein, dass entsprechende Daten vom Fahrzeug erhoben und bearbeitet werden.

Vernetzte Fahrzeuge haben Zugriff auf die Daten des Fahrzeugbesitzers, aber auch auf die Daten der Beifahrer. Das Auto kann nämlich auf die Daten aller zugreifen, die ihr Smartphone anschliessen (Kontaktdaten), aber auch auf Fahrzeugnutzungsdaten, wie etwa die GPS-Position, die Fahrzeit, die Abstellposition, die Zahl der elektromotorischen Gurtstraffungen und die Anzahl der verschiedenen Fahrer. Die erhobenen Daten sind nicht nur für den Garagisten zugänglich, der die Fahrzeugkontrollen durchführt, sondern werden auch regelmässig an den Fahrzeughersteller der jeweiligen Automarke übermittelt. Daraus kann geschlossen werden, dass unsere Daten je nach Automarke nicht gleich geschützt sind.

Die Daten von Autos europäischer Hersteller werden in Europa weitergegeben und bearbeitet, wo ein ähnlicher Datenschutz wie in der Schweiz besteht. Daten japanischer oder amerikanischer Automarken sind hingegen nicht unbedingt gleich gut geschützt, weil die Gesetzgebung dieser Staaten kein angemessenes Schutzniveau gewährleistet (siehe die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erstellte Liste der sicheren Staaten). So kann also nur schon die Wahl eines Fahrzeugs einen Einfluss auf die Nutzung unserer Daten haben. Einen Überblick über die Datenerhebung, -speicherung und –sendung gewisser Automarken erhalten Sie auf der Website des Verkehrsklubs ADAC unter folgender Adresse: https ://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/datenkrake_auto.aspx.

Neues aus dem Gesundheitsrecht

—

Den Neuerungen im allgemeinen Gesundheitsrecht ging die 24. Tagung des Gesundheitsrechts an der Universität Neuenburg nach.

Die Gesetzgebung zum elektronischen Patientendossier (ePD) ist am 15. April 2017 in Kraft getreten und ist wohl als wichtigste Neuerung im Bereich des Gesundheitsrechts zu bezeichnen. Dem Patienten ist freigestellt, ob er ein solches Dossier erstellen will oder nicht. Die Nutzung des ePD ist für Spitäler und Rehakliniken ab 2020 und für Heime und Geburtshäuser ab 2022 allerdings obligatorisch (siehe Resumé EPD). Wellen geschlagen hat auch der Entscheid des Europäischen Gerichtshofes für Menschenrechte vom 18. Oktober 2016 in Sachen Vukota-Bojic gegen die Schweiz. Der Gerichtshof hat festgestellt, dass die geheime Überwachung einer Rentenbezügerin durch einen Privatdetektiv die EMRK verletzt. Für eine solche Überwachung fehle die gesetzliche Grundlage (siehe: https://hudoc.echr.coe.int/eng#{«itemid»:[«001-167490»]})

Kommerzielle Medizin

Ein besonderes Augenmerk kam den neuen Strukturen für Gesundheitseinrichtungen zu. Einzel- und Kleinpraxen sind auf dem Markt immer weniger gefragt. Der Trend geht zu grösseren Strukturen, sei es in der Form der Aktiengesellschaft oder anderen privatrechtlichen Formen. Laut dem Neuenburger Kantonsarzt, Dr. Robert, stellt dieser Trend die Aufsichtstätigkeit vor neue Herausforderungen, die mit der vermehrten Mobilität von Gesundheitsfachpersonen, der Personenfreizügigkeit oder Diplomen ausländischer Bildungseinrichtungen zusammenhängen. Darüber hinaus setzen die kantonalen Zuständigkeiten einer wirksamen, kantonsübergreifenden Aufsicht Grenzen. Gerade im Zusammenhang mit der Wahrung der Patientenrechte – wie Zugangsrechte, Auskunftsrechte, Wahrung des medizinischen Berufsgeheimnisses – werden die Aufsichtsbehörden vermehrt angerufen. Die Durchsetzung dieser Rechte stösst denn auch vielfach auf Schwierigkeiten, die mit den privatrechtlichen und rein gewinnorientierten Strukturen einhergehen und nicht selten zu schneller Praxisaufgabe führen.

Funktioniert der Gesundheitsmarkt wie jeder andere Markt?

Für ein öffentliches Gesundheitswesen, das den qualitativen Anforderungen genügen soll, braucht es staatliche Regulierung und neue gesetzliche Grundlagen. Es braucht Ansätze, die geeignet sind, eine wirksame Aufsichtstätigkeit zu gewährleisten.

Elektronisches Patientendossier und Datenschutz

—

An einem Informationstag von privatim über das elektronische Patientendossier lag der Fokus auf der Funktionsweise und der Bedeutung des Vertrauens der Patientinnen und Patienten.

Elektronisches Patientendossier: Funktionsweise und besondere Risiken

Bei den elektronischen Patientendossiers (EPD) ist der Datenschutz wichtig, weil viele sensible Gesundheitsdaten von den Patienten selber, den Gemeinschaften und Stammgemeinschaften, den Gesundheitsfachpersonen und IT-Dienstleistern bearbeitet werden. Die Gesetzgebung über das EPD enthält neue Pflichten, welche die am EPD Beteiligten erfüllen müssen. Hauptsächlicher Rechtfertigungsgrund für das Bearbeiten von Daten im EPD ist die Einwilligung der Patienten. In der Verordnung sind verschiedene Arten von Einwilligungen vorgesehen, und zwar in Form von «Opt-In » (die betroffene Person muss ihre Einwilligung zur Bekanntgabe erteilen) oder «Opt-Out » (die betroffene Person muss tätig werden, um die Bekanntgabe zu verhindern). Gewisse Bestimmungen, die eine Einwilligung vom Typ «Opt-Out» vorsehen, sind datenschutzrechtlich problematisch, da sie den Gesundheitsfachpersonen einen Zugriff auf die Daten gewähren, obwohl diese sie für die Erfüllung ihrer Aufgabe nicht benötigen, was gegen den Grundsatz der Verhältnismässigkeit der Datenbearbeitung verstösst. Der Gesetzgeber hat trotz der von den Arbeitsgruppen von «eHealth» Schweiz geäusserten Bedenken an dieser Lösung festgehalten, mit dem Argument, die Einführung der «Opt-In»-Einwilligung könne die Verbreitung des EPD in der Gesellschaft beeinträchtigen.

Aufbau von Gemeinschaften und Stammgemeinschaften auf kantonaler Ebene

Die Gesetzgebung sieht eine dezentrale Einführung des EPD vor und definiert zu diesem Zweck «Gemeinschaften» und «Stammgemeinschaften» genannte Organisationseinheiten, die die organisatorischen und technischen Massnahmen umsetzen sollen und denen sich nur Gesundheitsfachpersonen anschliessen können. Hingegen ist nicht klar, wer für deren Bildung und Betrieb verantwortlich ist und wie die von den EPD verursachten Betriebskosten finanziert werden. Den Kantonen werden zwei Aufgaben übertragen: Sie prüfen die Finanzhilfegesuche des Bundes für den Aufbau einer Gemeinschaft/Stammgemeinschaft, geben eine Stellungnahme ab und sanktionieren die Dienstleister, die sich in Missachtung des Gesetzes keiner Gemeinschaft anschliessen. Die Kantone sind zudem für das Gesundheitsversorgungssystem für ihre Bevölkerung verantwortlich, dessen Effizienz und Qualität mit dem EPD verbessert werden soll, was die Kantone veranlasst, sich für die Einführung des EPD stark zu machen. Der Kanton Zürich schafft beispielsweise Rahmenbedingungen für eine rasche und flächendeckende Einführung des EPD.

Datenschutz und Datensicherheit in der Gesetzgebung zur Umsetzung des EPDG

Absolut sicher sind nur Daten, auf die nicht zugegriffen werden kann, allerdings sind sie dann aber auch nutzlos. Wichtig für eine gute Patientenversorgung ist die Verfügbarkeit der richtigen Informationen zum richtigen Zeitpunkt am richtigen Ort. Es braucht also eine Balance zwischen den Risiken der Informationsweitergabe und den Risiken fehlender Information. Das EPD ist fakultativ, die Patientinnen und Patienten müssen also unbedingt Vertrauen in dieses System haben können. Deshalb braucht es entsprechende Sicherheit, die aber auch ihren Preis hat. Die Balance für ein so komplexes System wie «eHealth» zu finden, bleibt für den Gesetzgeber eine Herausforderung; er muss Kompromisse zwischen Datenschutz und -sicherheit, Patientensicherheit, aber auch zwischen Kosten und Usability sowie zwischen Regelungsdichte und individueller Verantwortlichkeit finden. Zu diesem Zweck ist eine kontinuierliche und intensive Zusammenarbeit insbesondere zwischen den Fachverbänden, Patientenorganisationen und den Datenschutzbeauftragten für eine spezifische, effiziente und auf breite Akzeptanz stossende Regelung entscheidend.

Videoüberwachung am Arbeitsplatz

Ein Bäckereibetrieb erhob beim Kantonsgericht Beschwerde gegen die Nichterteilung einer Bewilligung für das Anbringen einer auf den Personaleingang gerichteten Videoüberwachungskamera mit Aufzeichnung. Das Kantonsgericht gab zu bedenken, dass der Sicherheitszweck einen besonderen Stellenwert haben muss, das heisst auf den Schutz des Lebens, der körperlichen Integrität oder den Schutz vor Vandalismus abzielt, damit die Videoüberwachung verhältnismässig ist. Die Überwachung muss angemessen sein, also ihren Zweck effektiv erfüllen und auf das dazu Notwendige beschränkt sein. An sich erfüllt die betreffende Installation, die den Parkplatz und den Personaleingang abdeckt, ihren Zweck, da sie abschreckend ist und Straftäter überführen kann, sie steht aber aus mehreren Gründen in keinem Verhältnis zum Bestimmungszweck. So steht einiges, was gefilmt wird, in keinem Zusammenhang mit dem Sicherheitszweck, und mit der Aufnahme des Personaleingangs kann beobachtet werden, wann die Angestellten kommen und gehen, mit wem sie sich unterhalten oder sich ein Fahrzeug teilen. Zudem gibt es beim betreffenden System keine direkte Kontrolle durch befugte Sicherheitsleute, und der Privacy-Filter schliesst die Gefahr einer Persönlichkeitsverletzung für die Angestellten nicht aus, weil die Aufnahmen nur an den Rändern, aber nicht im Zentrum verpixelt sind. Nicht betroffene Personen müssen schliesslich dem Aufnahmebereich der Kamera ausweichen können und eine andere Zugangsmöglichkeit haben, ohne sozusagen Totalüberwachung. Somit sind die Kameras, die schon im Innern des Gebäudes angebracht sind, für den Zweck der Verhinderung von Straftaten ausreichend, so dass das Entfernen der auf den Personaleingang gerichteten Kamera der abschreckenden Wirkung der Gesamtüberwachung keinen Abbruch tut. Das Kantonsgericht hat die Beschwerde abgewiesen (Urteil des Kantonsgerichts vom 18. Mai 2017, 601 2016 127).

Sensible Gesundheitsdaten für alle?

—

Die Digitalisierung und die neuen technologischen Entwicklungen machen auch vor den besonders schützenswerten Gesundheitsdaten nicht halt. «Quantified Self», ein Trend, unsere Gesundheitsparameter zu messen, oder «Blockchain» sind nur zwei von zahlreichen Beispielen der neuen Technologien. Wie steht es hier um den Datenschutz?

Die neuen Technologien erlauben immer mehr Gesundheitsdaten zu sammeln. Was geschieht mit ihnen? Der Ausgleich von Interessen des Konsumenten oder Patienten und jenen der Wirtschaftsakteure gerät zunehmend unter Druck. In der Politik wird der Ruf nach der Sozialpflichtigkeit von Gesundheitsdaten laut. Diesen Fragen ging im August das 22. Symposium on Privacy and Security in Zürich nach.

Ist die Datenbearbeitung transparent?

Die Bearbeitung von Gesundheitsdaten erfolgt nicht in einem rechtsfreien Raum. In einem ersten Beitrag wurde aufgezeigt, welche neuen datenschutzrechtlichen Erfordernisse das europäische Recht bringt. Einerseits sind es datenschutzfreundliche Voreinstellungen («privacy by default») oder datenschutzfreundliche Technik («privacy by design»). Auch sieht die Gesetzgebung neue Informations-, Dokumentations- und Meldepflichten (z.B. bei Databreaches) vor. Bund und Kantone müssen ihre Gesetzgebungen im Datenschutzrecht den Anforderungen des europäischen Rechts anpassen.
«Blockchain» ist eine verteilte Datenbank, die durch Kryptographie gesichert ist. Christian Cachin, Kryptographie- und Informatik-Forscher bei IBM, stellte in seinem Referat die Technik dar und erläuterte, dass sich aufgrund der breiten Verteilung der Datenbank die Transparenz unter den Teilnehmern erhöhe. Gleichzeitig hat dies allerdings zur Folge, dass die Daten breiter gestreut werden. Datenschutz und der Schutz der Persönlichkeitsrechte sind jedoch praktisch inexistent und es gibt kein Recht auf Vergessen.
«Quantified Self – Die Vermessung des Ichs» ist heute ein grosser Boom. Ziele dieser verschiedenen Applikationen und der mannigfaltigen Wearables (Smartphones, Smart Clothes, Hearables u.a.) sind die Selbstvermessung, ein Selbstmonitoring, eine bessere Selbsterkenntnis, aber auch Optimierung und Motivation. Man unterscheidet vier grosse Anwendungsbereiche: Smart Body, Smart Home, Smart Car und Smart Environment. Hier besteht ein grosses Missbrauchsrisiko. Denn die verschiedensten Applikationen erlauben dem Anbieter, das Nutzungsprofil der User zu erfassen. Häufig ist jedoch für den User nicht klar, was mit diesen Daten geschieht. Wie verwendet der Anbieter die Daten, verkauft er sie weiter und wenn ja, wem und für welche Zwecke? Daher der Aufruf von Herrmann Kollmar, Dr.med. und Dipl.Inform. bei Medgate: «Bleiben Sie Herr Ihrer Daten».

Klare Normen und Standards

Viele Daten zur Gesundheit werden auch im Arbeitsverhältnis erhoben, wie Rechtsanwalt Dr. Roger Rudolf aufzeigte. Die Fürsorgepflicht des Arbeitsgebers setzt allerdings der Datenbearbeitung Grenzen. Daten dürfen nur soweit erhoben werden, als sie für die technische Abwicklung wie auch für die Eignung notwendig sind.
In ihrem Referat stellte sich Prof. Dr. Franziska Sprecher gegen die Sozialpflichtigkeit von Gesundheitsdaten. Es brauche klare und transparente Normen und Standards, die es dem Patienten ermöglichen, selbst zu bestimmen, wem welche Daten preisgegeben werden. Dazu braucht es Sensibilisierung wie auch Vertrauen in eine transparente und sichere Datenbearbeitung.

Digitale Diktatur?

Die Panelteilnehmer waren sich einig, dass eine Sensibilisierung und die digitale Mündigkeit des Bürgers angestrebt werden müsse. Der betroffene Bürger müsse bewusst entscheiden können, wem er Daten anvertraut und welche er zu welchen Zwecken weitergibt.
Nach Milosz Matuchek, Jurist und Publizist, leben wir bereits heute in einer digitalen Diktatur, deren Folgen für den Bürger allerdings nicht ersichtlich seien. Die Digitalisierung werde häufig als alternativlos gesehen. Um diese negative Situation zu überwinden brauche es klare Kriterien für die Umschreibung von Fortschritt, Verbündete, aber auch eine digitale Bürgerwehr.

Informationen an öffentliche Organe

Auslagerung von Daten – Cloud Computing

Privatfirmen und öffentliche Organe lagern immer öfter die Bearbeitung ihrer Daten aus. Das heisst, sie beauftragen extern und gegen Bezahlung Dritte mit bisher intern erledigten Datenbearbeitungen. Meist wird dies mit wirtschaftlichen Gründen gerechtfertigt. Die weltweite Vernetzung und die Nutzung virtueller Speicher werfen aber viele Fragen auf: Weiss das öffentliche Organ bei einer Auslagerung, wo seine Daten hingehen, ob sie von Subunternehmern bearbeitet werden, ob sie angemessen geschützt werden und ob damit wirklich gespart werden kann? Für die Berechtigung zur Auslagerung muss das öffentliche Organ die gesetzlichen Pflichten erfüllen und insbesondere alle organisatorischen und technischen Massnahmen gegen jegliches unerlaubte Bearbeiten der Daten treffen. Ausserdem haftet es für die Risiken der Auslagerung, da es die für die Daten verantwortlich bleibt.

Die Kommission unserer Behörde hat ein Merkblatt über das Outsourcing von Daten des Staates in einer Cloud verfasst und auf die Risiken dieses Outsourcing und die strengen Auflagen hingewiesen. Es wird auch darauf hingewiesen, dass das öffentliche Organ für seine Daten verantwortlich bleibt. Die öffentlichen Organe müssen Transparenz schaffen punkto Bearbeiten von Daten der Bürgerinnen und Bürger, die keine andere Wahl haben, als ihre Daten an die Steuerverwaltung, die Einwohnerkontrolle, das Zivilstandsamt usw. weiterzugeben. Der Staat muss ihnen dafür die Sicherheit ihrer Daten garantieren, um sich ihr Vertrauen zu bewahren. Schliesslich verweist die Kommission auf das Gutachten von Wolfgang Wohlers, wonach bereits die Auslagerung von besonders schützenswerten Personendaten, wie auch von geheimen oder vertraulichen Daten in eine Cloud eine Verletzung des Amts- respektive des Berufsgeheimnisses darstellt.

Mehr dazu im Merkblatt über folgenden Link: http://intranet.fr.ch/intra/de/intra/functions/alle_news.cfm?fuseaction_pre=Detail&NewsID=62667

Anpassung der Verordnung über den Zugang zu Dokumenten

Nach dem Inkrafttreten des geänderten Gesetzes über die Information und den Zugang zu Dokumenten (InfoG) am 1. Januar 2017 tritt nun am 1. Januar 2018 die Verordnung über den Zugang zu Dokumenten (DZV) in ihrer angepassten Version in Kraft. Somit ist die ganze Freiburger Gesetzgebung im Transparenzbereich an die Aarhus-Konvention angepasst, die für die Schweiz am 1. Juni 2014 in Kraft getreten ist und der Öffentlichkeit im Umweltbereich in einigen Punkten ein weiter gefasstes Zugangsrecht gewährt als dasjenige, das allgemein im InfoG vorgesehen war.

Da im Gesetz der Grundsatz der Auslegung gemäss der Aarhus-Konvention eingeführt wurde, konnte auf mehrere Detailveränderungen in der DZV verzichtet werden. Gewisse Anpassungen waren aber trotzdem nötig, weil einerseits die vom Gesetzgeber gemachten Änderungen sich nicht auf den Umweltbereich beschränken, und sich andererseits die Verfahrensordnung geändert hat und auf Verordnungsebene festgelegt werden musste. Zudem wurden einige Anpassungen vorgenommen, welche die Erfahrungen der ersten 6 Jahre bei der Anwendung der Gesetzgebung über den Zugang zu Dokumenten berücksichtigen.

Da die DZV rund um die Begriffe der öffentlichen Organe im engen Sinn und der amtlichen Dokumente entworfen wurde, mussten zwei neue Bestimmungen eingeführt werden, um die Verbindung zum neuen Begriff der Privatpersonen, die öffentlichen Organen gleichgestellt werden, und zu demjenigen der Information über die Umwelt herzustellen. Dass der kantonalen Behörde für Öffentlichkeit und Datenschutz Entscheidungsbefugnis verliehen wird und für Gesuche um Zugang zu Informationen über die Umwelt besondere Fristen gelten, bilden ebenfalls Änderungen bei der Verfahrensordnung, die in der Verordnung konkret umgesetzt werden mussten.

Zu den Anpassungen, mit denen die Praxis berücksichtigt und die Arbeit der öffentlichen Organe vereinfacht werden sollen, gehört der erleichterte Zugang zu Dokumenten, die bereits in der Öffentlichkeit verbreitet wurden. Der Begriff fertig gestelltes Dokument wurde genauer umschrieben, so dass er auch Dokumente, die von Dritten stammen, umfasst, und die Liste der Ausnahmen von der Pflicht, betroffene Dritte anzuhören, wurde ergänzt und verdeutlicht. Schliesslich wurde eine neue Bestimmung hinzugefügt; sie betrifft die Pflicht der Parteien, in der Schlichtung mitzuwirken.

Der Verordnungsvorentwurf war in der Vernehmlassung im Sommer 2017 gut aufgenommen worden, und die vorgeschlagenen Änderungen waren insgesamt als notwendig und stichhaltig beurteilt worden. Alle Bemerkungen wurden von der Arbeitsgruppe genau geprüft, und viele von ihnen wurden auf die eine oder andere Art und Weise berücksichtigt.

Studie zu einheitlichem Personenidentifikator

–

Persönliche Daten, darunter oftmals sensitive Personendaten sind in der Schweiz in über 14000 administrativen und organisatorischen Registern gespeichert und mit einem einheitlichen Personenidentifikator, der AHV-Nummer indexiert. Diese Computersysteme sind anfällig auf Attacken durch verschiedene Angreifer. Ein neues Gutachten der ETH Zürich kommt zum Schluss, dass diese Risiken nicht unerheblich sind, da viele IT-Systeme von Schulen, Gemeindeverwaltungen oder Nichtregierungsorganisationen relativ unsicher seien. Es wird daher die Verwendung von sektorspezifischen Identifikatoren empfohlen, das heisst von nicht sprechenden Pseudonymen, und die Schaffung von Identifikationsprozessen, verbunden mit neuen Normen sowie einer wirksamen Kontrolle der Verknüpfungen. Das Gutachten finden Sie unter https://www.edoeb.admin.ch/aktuell/index.html?lang=de

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 2017