Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

datum

Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Dezember 2014

Inhalt

Editorial

Liebe Leserin, lieber Leser

Das Interesse an persönlichen Daten ist enorm, und viele der datengenerierenden Anwendungen und Dienstleistungen sind aus dem Alltag kaum mehr wegzudenken. Detailhändler ermitteln über Kundenkarten unsere Einkaufsgewohnheiten, um uns allerlei Schnäppchen schmackhaft zu machen, Onlineportale werten unsere Surf- und Kaufgewohnheiten aus, und in Autos eingebaute Rechner analysieren das Fahrverhalten der Lenker. Mit der Auswertung persönlicher Internetdaten sollen jährlich geschätzte dreistellige Milliardenbeträge umgesetzt werden. Auch vor dem Gesundheitsbereich hat der Datensammelboom nicht haltgemacht. Mit GesundheitsApps auf dem Smartphone, Schrittzählern und Fitnessarmbändern messen immer mehr Leute ihre Aktivitäten und Körperfunktionen rund um die Uhr und geben ihre Daten preis. Die Akteure im Gesundheitsbereich haben ein reges Interesse an diesen Informationen. – Weil der Umgang mit persönlichen Daten gerade im Gesundheitsbereich heikel ist, möchten wir ihn hier kritisch beleuchten.

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Silvia Böhlen
Redaktionsverantwortliche

Themen

Folgen der digitalen Selbstvermessung

Der technologische Fortschritt findet gerade im Gesundheitsbereich offene Türen. Von der medizinischen Forschung bis in den Alltag eröffnen sich ungekannte Möglichkeiten. Unmengen von Gesundheitsdaten werden von verschiedensten Interessengruppen gesammelt, gespeichert und vielfältig ausgewertet. Auch die Behörden haben ein grosses Interesse an den Daten, die wir dank des Trends zur Selbstvermessung bereitwillig zuliefern. Dass es sich dabei um sensible Personendaten handelt, ist uns oft zu wenig bewusst. Eine amerikanische Studie kam 2013 zum Schluss, dass der Grossteil der FitnessApps keinen genügenden Datenschutz bietet, um eine vertrauliche Datenbearbeitung zu gewährleisten. Der EDÖB verfolgt die Entwicklung deshalb aufmerksam und möchte in der Folge einige Aspekte aus Datenschutzsicht kritisch beleuchten.

Quantified Self

Der Trend zur Selbstvermessung des eigenen Körpers mittels Sensoren in Armbändern, Schrittzählern oder gar Kontaktlinsen dient dem Erkenntnisgewinn zu persönlichen, sportlichen, gesundheitlichen und gewohnheitsspezifischen Fragestellungen. Hinter der guten Absicht, Verantwortung für den eigenen Körper zu übernehmen und gesünder zu leben, lauern aus Datenschutzsicht aber beachtliche Gefahren: Menschen, die sich selber permanent vermessen und statistisch auswerten, häufen gewaltige Datenmengen an, die sie kaum mehr überblicken können. Und wenn jemand die Herrschaft über seine eigenen Daten und die daraus gezogenen Schlüsse verliert, wird das Grundrecht auf

informationelle Selbstbestimmung unterlaufen und die Prinzipien des Datenschutzgesetzes infrage gestellt.

Interessen Dritter

An den Daten, die wir mit GesundheitsApps und Wearables generieren und die Aufschluss über unseren Gesundheitszustand bzw. allfällige Krankheiten geben, haben nebst den Akteuren im Gesundheitsbereich auch andere Wirtschaftszweige ein grosses Interesse. Für die Betroffenen ist das sehr heikel, da bspw. Angaben zu Fettanteil, Schlafverhalten, Herz- oder Atemfrequenz Rückschlüsse auf den Gesundheitszustand und allfällige Krankheiten einer Person zulassen und dieser zum Nachteil werden können (z.B. Prämienerhöhungen oder Schwierigkeiten beim Versicherungsabschluss oder bei der Stellensuche). Es ist deshalb wichtig, dass jede Person frei entscheiden kann, ob und wem sie ihre Daten zur Verfügung stellen will (Recht auf informationelle Selbstbestimmung).

Manche Anbieter bedingen sich in den Geschäftsbedingungen das Recht aus, die Daten zu kommerziellen Zwecken weiterzuverwenden (bzw. an Dritte zu verkaufen). Es liegt in unserer Eigenverantwortung, Vor- und Nachteile der Selbstvermessungstools abzuwägen und die Seriosität des Anbieters zu prüfen (AGB und Datenschutzbestimmungen lesen!). Wir sollten uns bewusst sein, dass sich ein Fremdzugriff oder gar eine Manipulation der Daten nie ganz ausschliessen lässt.

Medizin 2.0: Neues Verhältnis Arzt – Patient

Durch Selbstvermessung können wir unsere medizinischen Werte wie Blutdruck, Cholesterin oder Blutzucker selber messen und kontrollieren und bis zu einem gewissen Grad vielleicht sogar selber steuern. Patienten können den Eindruck erhalten, selber alles im Griff zu haben und sich selber besser zu kennen als der Arzt, was zu einem Paradigmenwechsel in der Medizin führen könnte: weg von reaktiven Behandlungsmethoden, hin zu einer personalisierten, partizipativen Präventivmedizin. Diese Entwicklung kann sowohl aus datenschutzrechtlicher als auch aus medizinischer Sicht problematisch sein (Gefahr der Übertherapie, aber auch der falschen oder fehlenden Behandlung).

Betriebliche Gesundheitsförderung

Der Trend zur Selbstvermessung findet auch in der Arbeitswelt vermehrt Einzug. Denn gesunde, fitte Mitarbeitende sind auch leistungsfähiger. Mit Programmen wie „Bike to work" oder der Schaffung von Anreizen zum Beispiel durch Abgabe von Schrittzählern, kann das Verhalten der Arbeitnehmenden kontrolliert und gesteuert werden. Auch wenn die Teilnahme an solchen Programmen freiwillig bleibt, besteht die Gefahr der Benachteiligung und Diskriminierung. Betriebliche Gesundheitsförderung sollte deshalb nicht an einzelnen Aktionstagen oder -wochen aufgehängt werden, sondern vielmehr auf einem nachhaltigen, glaubwürdigen Wandel der gesamten Unternehmenskultur beruhen, die allen Mitarbeitenden etwas zu bieten hat.

Tipps des EDÖB

Mit der Nutzung von Wearables und GesundheitsApps geben wir nicht nur vielfältige Informationen über unsere Gesundheit preis, sondern kreieren auch ein aufschlussreiches Persönlichkeitsprofil. So lässt sich z.B. anhand der Aufzeichnung unserer

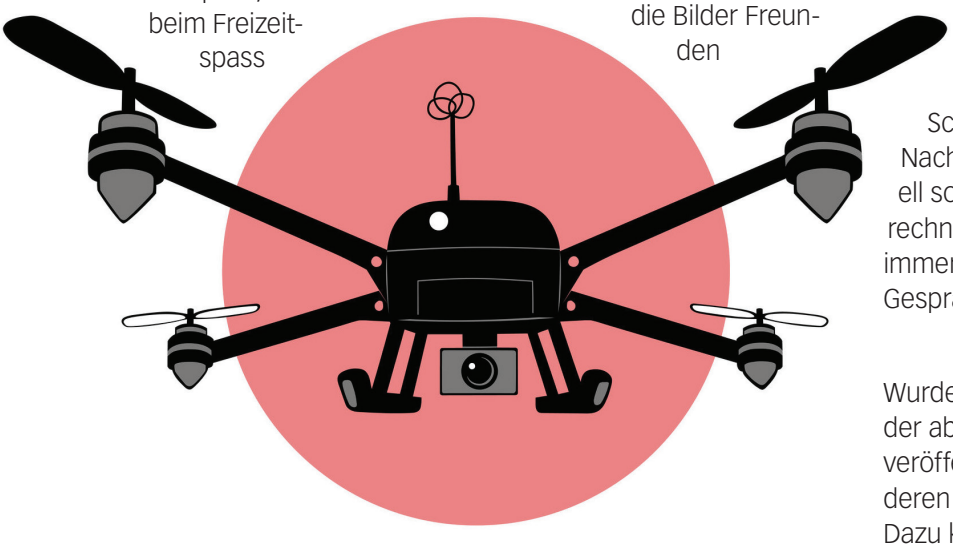
Schlafgewohnheiten auf unser psychisches Befinden schliessen. Die Gefahr, dass solche Informationen bei einer Versicherung oder dem Arbeitgeber landen, lässt sich nie ganz ausschliessen. Was aber tun, um bei der digitalen Selbstvermessung keine bösen Überraschungen zu erleben? Als Erstes empfiehlt sich ein Blick in die AGB oder Datenschutzbestimmungen – dort sollte drin stehen, wozu die Daten verwendet und ob sie an Dritte weitergegeben werden. Hat man sich für die Verwendung einer GesundheitsApp oder ähnlichem entschieden, ist es ratsam, eine möglichst datenschutzfreundliche Einstellung zu wählen und der Anwendung nur Zugriff auf Daten zu gewähren, die für die Erbringung des Zwecks erforderlich sind (und nicht etwa auf das Adressbuch, den Kalender oder Standortdaten).

Quellen:

- „Die vermessene Gesundheit", Beobachter, 16. Mai 2014
- „Le corps, nouvel objet connecté", CNIL, Cahiers IP 2-2014
- „Mobile Health and Fitness Apps: What Are the Privacy Risks?", Studie von Privacy Clearing Rights, 2013
- Interview zu Big Data in der Zeitschrift Die Volkswirtschaft 5-2014
- Erläuterungen zu Big Data auf der Internetseite des EDÖB

Drohnen, Dashcams & Co.

Eine Drohne im Garten fliegen zu lassen und damit auch mal über den Zaun zum Nachbar zu blicken, kann verlockend sein. – Da Drohnen immer billiger werden und einfacher zu handhaben sind, nimmt deren Einsatz im Privatbereich zu. Wenn sie mit einer Kamera bestückt sind, kommt ihr Einsatz einer Videoüberwachung gleich, bei der die Bestimmungen des Datenschutzgesetzes zu berücksichtigen sind. Ein Merkblatt auf unserer Website liefert detaillierte Informationen und praktische Beispiele, worauf beim Freizeitspass mit einer Drohne zu achten ist. Wir empfehlen Ihnen, einen Blick darauf zu werfen, bevor Sie mit Ihrem Multikopter die Nachbarn verärgern oder unbedarfte Passanten erschrecken!



Datenschutzproblematik von Drohnen

Oft sind sich die Betreiber gar nicht bewusst, dass sie etwas Unrechtmässiges tun, wenn sie mit einer Drohne in Bereiche eindringen, zu denen man zu Fuss keinen Zutritt hätte. Wenn sie die Bilder Freunden und Bekannten zeigen oder gar im Internet veröffentlichen, kann das die abgebildeten Menschen in ihrer Persönlichkeit verletzen.

Personen, die sich von einer Drohne belästigt fühlen und den Betreiber kennen, raten wir, diesen aufzufordern, damit aufzuhören und bereits erstellte Bilder zu löschen. Ohne Einwilligung der Betroffenen dürfen grundsätzlich keine Aufnahmen gemacht werden. Gegen einen Drohnenpiloten, der Personen heimlich filmt, kann Zivilklage erhoben werden; bei Verletzung des Geheim- oder Privatbereichs (z.B. wenn jemand durchs Schlafzimmerfenster des Nachbars filmt) muss er eventuell sogar mit einer Strafanzeige rechnen. Wir empfehlen aber immer, zuerst das persönliche Gespräch zu suchen.

Wurden Bilder ohne Einwilligung der abgebildeten Personen veröffentlicht, können diese deren Entfernung verlangen. Dazu können sie sich entweder

an den Urheber oder an die entsprechende Publikationsstelle wenden, beispielsweise an den Betreiber des Onlinedienstes, auf dem die Aufnahmen zu sehen sind. - Gänzlich unproblematisch sind die Aufnahmen nur dann, wenn auf ihnen keine Personen zu erkennen sind. Dies gilt natürlich auch für die anderen Formen von Videoüberwachung.

Dashcams

Wachsender Beliebtheit erfreuen sich auch die sogenannten Dashcams. Dabei handelt es sich um kleine Videokameras, die in Fahrzeugen angebracht werden und in der Regel dazu dienen, andere Verkehrsteilnehmer zu Beweiszwecken zu filmen. Der Umstand, dass diese die Kamera in der Regel nicht erkennen können und somit ohne ihr Wissen gefilmt werden, ist aus Sicht des Datenschutzes problematisch. Hinzu kommt, dass die Kameras meistens dauerhaft filmen und auch Fahrzeuge und ihre Insassen erfassen, die nichts mit einem allfälligen Ereignis zu tun haben. Ein solcher Gebrauch der Dashcam führt unweigerlich zu Persönlichkeitsverletzungen, wogegen die betroffenen Personen zivilrechtlich vorgehen können. Auch das wahllose Filmen sämtlicher Verkehrsteilnehmer mit dem Ziel, die Aufnahmen nach Verkehrsregelverstössen zu durchsuchen und die Fehlbaren anzuzeigen, ist in der Regel nicht zulässig. Die Ahndung der Fehlbaren und das Filmen im öffentlichen Raum (sprich auf der Strasse) ist in erster Linie Sache der Polizei. Statthaft sind Dashcam-Aufnahmen einzig dann, wenn ein überwiegendes öffentliches Interesse vorliegt. Dies kann dann der Fall sein, wenn sie den Hergang eines grösseren Unfalls oder einen gravierenden Verstoss gegen das Strassenverkehrsrecht festhalten. Über die Zulassung der Bilder als Beweismaterial entscheidet letztlich der Richter. Der Entscheid resultiert aus der Interessenabwägung zwischen Persönlichkeitsschutz und öffentlichem Interesse. Ausführliche Informationen zu den datenschutzrechtlichen Aspekten von Dashcams finden Sie auf unserer Webseite.

Videoüberwachung – gewusst wie!

Anders ist die Situation beim Einbruchschutz. Wer in den Urlaub fährt und Sorge vor Einbrechern hat, darf die eigenen vier Wände während seiner Abwesenheit filmen. Ein überwiegendes (privates) Interesse kann hier als Rechtfertigungsgrund für die Videoüberwachung geltend gemacht werden. Nachbarn, die die Wohnung während dieser Zeit betreten, beispielsweise um Blumen zu giessen, oder die Putzfrau, gilt es vorgängig zu informieren. Vorsicht ist auch bei öffentlich zugänglichen Bereichen eines Privatgrundstücks geboten. Wird ein Gehweg im Garten videoüberwacht, den z.B. der Postbote auf dem Weg zum Briefkasten benutzt, muss ein gut sichtbares Hinweisschild angebracht werden. Wenn tatsächlich ein Einbruch geschieht und dokumentiert werden kann, ist das Material der Polizei zu übergeben. Wenn kein Ereignis vorliegt, müssen die Daten innert 24 Stunden gelöscht werden, wenn Personen darauf zu erkennen sind. Bei der Installation der Kamera ist darauf zu achten, dass ihr Fokus nur auf das eigene Grundstück gerichtet ist. Den öffentlichen Raum oder das Grundstück des Nachbarn zu filmen, ist grundsätzlich widerrechtlich.

Über die zunehmende Tendenz zur flächendeckenden Videoüberwachung in Restaurants haben wir in unserem letzten Newsletter ausführlich berichtet. Der EDÖB hat in der Zwischenzeit in mehreren Betrieben, die systematische Videoüberwachung durchführten, Kontrollen durchgeführt und Verbesserungen insbesondere für die Arbeitnehmenden erzielt.

Weiterführende Informationen:

- Pressemitteilung des EUGH, 11.12.2014
- Urteil des Europäischen Gerichtshofs: Vorsicht bei Überwachungskameras vor eigenem Haus, Spiegel Online, 11. Dezember 2014
- Urteil des Gerichtshofs der Europäischen Union: Die Datenschutzrichtlinie gilt auch für Kameras zur Überwachung von Wohnhäusern, die auf den öffentlichen Straßenraum gerichtet sind, Nationale Kommission für den Datenschutz Luxemburg, 11.12.2014
- Les drones bourdonnent dans le ciel, Tout compte fait No 10, 22.10.2014
- Besorgter Autofahrer spielt Autobahn-Polizei, Luzerner Zeitung, 16.9.2014
- Dürfen wir in der Tiefgarage eine Videokamera installieren? Luzerner Zeitung, 28.8.2014
- 1:0 für den Datenschutz: Deutsches Gericht missbilligt Dashcam, SRF Espresso, 14.08.2014

Aus der Presse

Bundesverwaltungsgericht gewährt volle Einsicht in Dokumente zu Nachtflugmonitoring – Rekurs gegen EDÖB-Empfehlung abgewiesen

Der Schutzverband der Bevölkerung um den Flughafen Zürich (sbfz) darf alle Dokumente zum Nachtflugmonitoring des Bundesamts für Zivilluft¬fahrt (BAZL) einsehen. Dies geht aus einem Entscheid des Bundesverwaltungsgerichts vom 28. Oktober 2014 hervor (A-6291/2013). Das Gericht kommt somit zum selben Schluss wie der EDÖB, der in seiner Empfehlung vom 17. September 2013 das BAZL aufgefordert hatte, dem Verband Einsicht in sämtliche Monitoring-Dokumente zu geben, namentlich in Sitzungsprotokolle und in ein Dokument mit „Entscheidhilfen" für Ausnahmebewilligungen. Der Argumentation des BAZL, wonach die verweigerten Unterlagen keine amtlichen Dokumente darstellten, folgte das Gericht nicht. - Das 2010 vom BAZL eingeführte Monitoring sollte Auskunft geben, wie beim Flughafen Zürich Ausnahmebewilligungen für Nachtflüge erteilt werden.

Quelle:

- Flughafen-Schutzverband darf Dokumente zu Nachtflugmonitoring sehen. SDA, 06.11.2014

Tipps

Was gilt es bei Social Media zu beachten?

- Gleich bei der ersten Anmeldung Privatsphäre-Einstellungen überprüfen und anpassen (Die Standardeinstellungen der Anbieter beschränken den Datenschutz auf ein Minimum und lassen die Weiterverwendung der Daten durch Dritte oft zu)
- Allgemeine Geschäftsbedingungen hinsichtlich Datenschutz bzw. Weitergabe an Dritte gündlich durchlesen
- Onlinedienste nicht als private E-Mail-Dienste verwenden
- Telefonnummer und Adresse nicht im Profilsteckbrief publizieren
- Verunglimpfungen Dritter, Nacktfotos oder erniedrigende Bilder über sich selbst oder andere unterlassen
- auf Textnachrichten, Videos oder Bilder, die Rückschlüsse auf die politische oder religiöse Gesinnung zulassen, verzichten
- Für die Übertragung von sensiblen Informationen verschlüsselte E-Mail (Meldung sowie Anhänge) verwenden. (Google hat zwar angekündigt, den Verkehr zwischen den E-Mail-Servern mit SSL-Verschlüsselung abzusichern. Dies ist jedoch nur möglich, wenn beide beteiligten Server diesen Standard erlauben.)

Quelle:

- Dos und Don'ts im Umgang mit Sozialen Medien. Luzerner Zeitung, 12.06.2014.

Weitere Informationen:

- www.derbeauftragte.ch > Datenschutz > Soziale Medien > Erläuterungen zu Sozialen Netzwerken

Löschung von Spuren im Netz

Daten zu Ihrer Person können auf verschiedenen Wegen gegen Ihren Willen ins Internet gelangen und somit öffentlich zugänglich werden. Wenn Sie selber keine Daten über sich im Netz publizieren, vermeiden Sie bereits einen Grossteil von möglichen Veröffentlichungen. Ihre Daten können aber auch aus Quellen Dritter (z.B. aus Telefonverzeichnissen) ins Netz geraten. Sie können von Zeit zu Zeit prüfen, ob Informationen über Sie im Internet auftauchen

und diese gegebenenfalls löschen lassen. Eine umfassende Löschung der Inhalte sollte primär bei der „Quelle" durchgesetzt werden, d.h. beim Betreiber einer bestimmten Website oder beim Inhaber eines Social-Media-Profils. Reagiert dieser nicht, kann man beim Suchmaschinenanbieter die Entfernung des entsprechenden Links aus den Suchergebnissen verlangen, die Inhalte bei der Primärquelle bleiben in diesem Fall aber erhalten.

Literaturhinweis

Weber , Rolf H. /Thouvenin, Florent (Hrsg.): Big Data und Datenschutz - Gegenseitige Herausforderungen, Zürich, 2014

Mayer-Schönberger, Viktor/Cukier, Kenneth: Big Data. Die Revolution, die unser Leben verändern wird. Redline-Verlag, München, 2013

Hofstetter, Yvonne: Sie wissen alles. Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen, München, 2014

Agenda

Weiterbildung Datenschutzrecht: 8. Mai 2015

Datenschutz und Videoüberwachung
Institut für Europarecht, Universität Fribourg

In eigener Sache

Internationaler Datenschutztag: 28. Januar 2015, 10-12 Uhr, in Bern

Podiumsdiskussion des EDÖB mit ausgewählten Vertretern aus Politik, Wissenschaft und Wirtschaft zum Thema «GesundheitsApps und Wearables - eine Bedrohung für die Privatsphäre?»

Anmeldung www.derbeauftragte.ch oder info@edoeb.admin.ch

Teilen Sie Ihre Meinung im Blog
www.blog.edoeb.admin.ch

datum ist eine Publikation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und erscheint zweimal jährlich.

Impressum

Dezember 2014

Übersetzungen: Schweizerische Bundeskanzlei, Sprachdienste

Dieser Newsletter ist auch auf Französisch und Italienisch erhältlich.

Der EDÖB im Internet: www.derbeauftragte.ch