Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

datum

Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

August 2016

Inhalt

Editorial

Liebe Leserin, lieber Leser,

Weil ein Tag nur 24 Stunden zählt, ist es manchmal schwierig, alles unter einen Hut zu bringen: Nach der Besprechung bei einem Kunden am Vormittag reicht die Mittagspause gerade für einen sommerlichen Kurzhaarschnitt bevor ich um zwei Uhr zur Teamsitzung hasten muss. – „Treffen wir uns zum Feierabendbier?“, fragt ein Kumpel während mir der Frisör den Nacken ausrasiert. „Na klar, gute Idee!“, smse ich zurück und schon steht ein weiterer Termin in meiner digitalen Agenda. Zum Glück erinnert mich mein Smartphone zuverlässig jeweils eine halbe Stunde vor einer Verabredung daran. Die praktischen Helfer im Alltag sind auch aus der Arbeitswelt nicht mehr wegzudenken. Wenn aber das Risiko besteht, dass Geschäftliches und Privates vermischt werden, gerät auch unsere Privatsphäre in Gefahr.

Vielleicht ziehen wir nach dem Feierabendbier noch weiter und landen kurz vor Mitternacht in einer feuchtfröhlichen Party. Dann sollten wir lieber kein Erinnerungs-Selfie in einem sozialen Netzwerk posten. – „Was wird mein Vorgesetzter von mir denken, dessen Freundschaftsanfrage ich mich neulich nicht wegzudrücken getraut habe…?“ Ist ein Foto einmal online, sieht es die ganze Welt! Kompromittierende Bilder im Internet können zum vorzeitigen Ausscheiden in einem Bewerbungsprozess führen, in gravierenden Fällen sogar zu einem Jobverlust. – Wäre es nicht interessant zu wissen, was in der Personalakte meines Arbeitgebers alles über mich steht?

Aus der zunehmenden Digitalisierung von Arbeit und Freizeit resultieren verschiedene Gefahren aus Sicht Datenschutz. Der vorliegende Newsletter thematisiert den Arbeitsbereich und will Arbeitgeber und Arbeitnehmer auf Rechte und Pflichten im Bereich Datenschutz hinweisen.

Silvia Böhlen
Redaktionsverantwortliche

Personaldossier - Was darf ein Arbeitgeber wissen?

Die Digitalisierung vereinfacht das Sammeln von Daten auch im Personalwesen, sei es im Bewerbungsprozess oder während des Arbeitsverhältnisses. Zwar darf ein Arbeitgeber nur Personendaten bearbeiten, die für die Ausführung eines bestimmten Jobs erforderlich sind. Findet er aber Daten über einen Bewerbungskandidaten oder eine Mitarbeiterin im Internet, kann ihm das kaum vorgeworfen werden. Mitarbeitende können jederzeit Auskunft über die sie betreffenden Daten verlangen und falsche Einträge berichtigen oder löschen lassen.

Sowohl vor als auch nach Vertragsabschluss darf ein Arbeitgeber nur Mitarbeiterdaten bearbeiten, „soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind“, schreibt das Obligationenrecht vor. Informationen, die durch eine einfache Suche im Internet gefunden werden, können aber auch einem Arbeitgeber kaum verheimlicht werden. Wenn kompromittierende Beitrage in sozialen Netzwerken zum Ausscheiden in einem Bewerbungsprozess oder gar zu einem Jobverlust führen, ist der betroffene Arbeitnehmer bzw. die Arbeitnehmerin selber dafür verantwortlich. Es bleibt allerdings zu hoffen, dass er oder sie die Möglichkeit erhält, persönlich zu den fragwürdigen Inhalten Stellung zu nehmen und der Arbeitgeber das persönliche Gespräch höher bewertet als die Informationen aus dem Internet.

Immer öfter wird heute von den Bewerbungskandidaten ein Strafregisterauszug verlangt, was in verschiedener Hinsicht fragwürdig, und in vielen Fällen schlicht unverhältnismässig ist. Ein Strafregisterauszug darf nur verlangt werden, wenn eine Funktion dies absolut erfordert, was im Einzelfall zu beurteilen ist. Wenn diese Daten für das Arbeitsverhältnis nicht relevant sind, ist das automatische Einfordern eines Strafregisterauszugs aus Datenschutzsicht unzulässig. Es verstösst ausserdem gegen das dem Schweizer Strafsystem zugrundeliegende Resozialisierungsprinzip. Ein Strafregisterauszug ist lediglich eine Momentaufnahme und keine Garantie dafür, dass sich eine bestimmte Person noch nie etwas hat zu Schulden kommen lassen. Viel wichtiger ist deshalb das persönliche Kennenlernen der Kandidaten im Vorstellungsgespräch.

Besondere Vorsicht ist im Umgang mit Gesundheitsdaten geboten, da sie als besonders schützenswerte Personendaten gelten. Ein Arbeitgeber darf beispielsweise keine Auskunft über den Gesundheitszustand verlangen. Wenn ein Arbeitnehmer einen Gesundheitsfragebogen ausfüllen muss, dürfen die erhobenen Daten nur von einem Vertrauensarzt analysiert werden. Selbst dieser darf Dritten keine Auskunft zu einer Diagnose eines Patienten geben. Er darf einem Arbeitgeber lediglich mitteilen, ob der Gesundheitszustand eines Patienten erlaubt, eine bestimmte Tätigkeit auszuüben. Auch Programme zur betrieblichen Gesundheitsförderung können datenschutzrechtlich heikel werden, wenn der Arbeitgeber auf diesem Weg zu Informationen über den Gesundheitszustand seiner Angestellten kommt.

Gefahren der Digitalisierung

Heute übernimmt oft eine Personalsoftware die Verwaltung der Mitarbeiterdaten. Es gibt Programme, die auch als Kommunikationsplattform genutzt werden und den Austausch zwischen Unternehmen und Mitarbeitern verbessern können, was einen positiven Effekt auf die Zufriedenheit und das Engagement haben kann. Manche Programme, die wohl vor allem für Grossunternehmen interessant sein dürften, ähneln sozialen Netzwerken und erlauben den Angestellten, ihre Profile selber zu verwalten und mit persönlichen, auch privaten Informationen zu speisen. Bei solcher Personalsoftware erkennen Algorithmen aus Personaldaten nicht nur Muster und geben aufgrund von früher gemachten Erfahrungen spezifische Empfehlungen ab, sie können HR-Managern auch dazu dienen, intern die richtigen Personen für bestimmte Projekte zu finden. Der Vorteil solcher Programme ist, dass sie die Gesamtheit der vorhandenen Informationen in die Evaluation einbeziehen und ohne Vorurteile auswerten. Aus Datenschutz-

sicht heikel kann es werden, wenn mittels Algorithmen das Verhalten der Mitarbeitenden analysiert wird und Persönlichkeitsprofile erstellt werden.

Weil die Datensammelei auch im Personalwesen Einzug hält, ist es wichtig, dass sowohl Arbeitgeber als auch Arbeitnehmer ihre Rechte und Pflichten im Bereich Datenschutz kennen. Ein Arbeitgeber darf nur Daten über seine Angestellten bearbeiten, die zur Erfüllung des Arbeitsvertrages erforderlich sind. Werden bestimmte Daten gezielt zur Durchführung von Aktionstagen im Rahmen der betrieblichen Gesundheitsförderung erhoben, sind diese danach wieder zu löschen. Ohne Einwilligung der betroffenen Personen dürfen die Daten weder an Drittpersonen weitergegeben noch für kommerzielle oder andere Zwecke verwendet werden. Ein Arbeitnehmer kann jederzeit Auskunft über alle durch den Arbeitgeber gesammelten ihn betreffende Daten verlangen, sei dies während oder nach Beendigung des Arbeitsverhältnisses, und gegebenenfalls sein Widerspruchsrecht geltend machen. Ein Auskunftsbegehren wird in der Regel schriftlich gestellt und muss nicht begründet werden.

Weiterführende Informationen:

- Aus dem 22. Tätigkeitsbericht (2014/2014) des EDÖB:
  - Gesundheitsfragebogen bei Bewerbungsverfahren
  - Referenzauskünfte im Bewerbungsprozess
- Newsletter 2012: Arbeitgeber-Recherchen in Sozialen Netzwerken
- Musterbriefe für Auskunfts-, Löschungs- und Berichtigungsbegehren

Quellen:

- Firmen sind zu neugierig. Beobachter, 8.7.2016
- „Computer kennen keinen Nasenfaktor". Frankfurter Allgemeine, 9.4.2016
- Die Mär des Strafregisterauszugs. Neue Zürcher Zeitung, 5.4.2016
- Einsicht in die Personalakte. Zürcher KMU, 1.4.2016

Überwachung am Arbeitsplatz - Privatsphäre auch während der Arbeit

Neue Arbeitszeitmodelle ermöglichen eine massgeschneiderte Work-Life-Balance. Doch auch wenn Vorgesetzte ihren Mitarbeitenden mehr Freiheit in der Gestaltung ihrer Arbeitszeiten gewähren, können sie sich dank digitaler Datenströme ein präzises Bild darüber erstellen, wann und wie lange die Beschäftigten auf welchen Kanälen aktiv sind: Die Digitalisierung schafft neue Möglichkeiten der Leistungskontrolle und Überwachung.

Beim Arbeiten hinterlassen die Beschäftigten zunehmend digitale Spuren, nicht nur wenn sie am Computer arbeiten und mit dem hauseigenen Server verbunden sind oder im Internet surfen. Wenn jemand an der Kasse eines Verkaufsladens arbeitet, die mit einer Kamera überwacht wird, oder als Chauffeur eines Handwerkbetriebs mit dem Dienstfahrzeug unterwegs ist, das mit einem Fahrtenschreiber oder GPS-Ortungssystem ausgerüstet ist, kann es zu Unstimmigkeiten zwischen Unternehmern und Angestellten kommen, wenn sich diese in ihrer Privatsphäre eingeschränkt fühlen. Darf eine Arbeitnehmerin oder ein Arbeitnehmer das Dienstfahrzeug auch privat nutzen, muss der Fahrtenschreiber nach Arbeitsende deaktiviert werden können. Wir empfehlen Arbeitnehmerinnen und Arbeitnehmern, die sich durch Überwachungsmassnahmen am Arbeitsplatz unter Druck gesetzt fühlen, das persönliche Gespräch mit dem Vorgesetzten zu suchen. Andernfalls können sie sich an das kantonale Arbeitsinspektorat wenden.

Leistungs- und Verhaltenskontrollen in Unternehmen dürfen grundsätzlich nur erfolgen, wenn das Personal klar darüber informiert worden ist. Arbeitgeber müssen sich auch die Frage stellen, welche technischen und organisatorischen Massnahmen sie zur Verhinderung von Missbräuchen ergreifen können. Ausserdem sollten sie ihren Angestellten klar kommunizieren, in welchem Rahmen die private Nutzung von Internet und E-Mail gestattet ist. Privates Surfen wird oft toleriert, soweit es das Erfüllen der arbeitsvertraglichen Verpflichtungen nicht behindert. Je nach Tätigkeitsbereich kann privates Mailen und Surfen vollständig verboten werden. Durchsetzung und Kontrolle eines Totalverbots sind jedoch mit grossem

Aufwand verbunden. Für eine ausführliche und transparente Information empfehlen wir den Erlass eines Nutzungsreglements. Je klarer das Nutzungsreglement ist, desto besser weiss die Belegschaft, was erlaubt und was verboten ist. Unnötigen Streitigkeiten kann damit Vorschub geleistet werden.

Massvolle Online-Überwachung erlaubt

Wenn keine anderslautende Regelung besteht, ist eine massvolle private Internetnutzung während der Arbeitszeit erlaubt. Die Kontrollmöglichkeiten durch den Arbeitgeber sind beschränkt. Der Einsatz von spezifischer Überwachungssoftware (z.B. Key-Logger) oder Content Scannern ist aus Datenschutzsicht heikel, da er zur Verhaltensüberwachung führen kann. Das Verbot der Verhaltensüberwachung gilt aber nicht absolut. Bei einem festgestellten Missbrauch oder einem begründeten Verdacht kann eine personenbezogene Auswertung rechtmässig (sprich verhältnismässig und zweckmässig) sein. Eine systematische Überwachung wäre aber höchstens in Betrieben mit erhöhten Sicherheitsanforderungen wie Banken oder Militär denkbar und müsste im Einzelfall beurteilt werden.

Das Bundesgericht hat eine fristlose Kündigung für unrechtmässig erklärt, weil ein Unternehmen auf dem PC eines Mitarbeiters heimlich eine Software installiert hatte, um nachweisen zu können, dass er zu viel Zeit für private Zwecke im Internet gesurft hatte. Erlaubt ist grundsätzlich nur eine anonymisierte Überwachung, wenn die Angestellten im Voraus klar darüber informiert worden sind, bspw. in einem Reglement oder in einer Weisung.

Um die Versuchung von übermässigem privaten Surfen einzuschränken und die Gefahr, dass dabei Viren, Trojaner oder andere Computerwürmer eingeschleust werden, zu minimieren, empfehlen wir präventive Massnahmen wie das Blockieren bestimmter gefährlicher Internetseiten, die Verwendung einer wirkungsvollen Antivirus-Software und die regelmässige Aktualisierung des Browsers. Eine Sensibilisierung der Angestellten für einen massvollen Internetkonsum sollte ebenfalls stattfinden.

Weiterführende Informationen:

- Leitfaden über die Bearbeitung von Personendaten im Arbeitsbereich
- Leitfaden Internet- und E-Mail-überwachung am Arbeitsplatz
- Erläuterungen zur Videoüberwachung am Arbeitsplatz
- Erläuterungen zur Telefonüberwachung am Arbeitsplatz
- Aus dem 22. Tätigkeitsbericht (2014/2015) des EDÖB: Sachverhaltsabklärung zu Videoüberwachung in Restaurants und Take-aways
- Medienmitteilung zum Bundesgerichtsentscheid vom 17. Januar 2013 „Ungerechtfertigte fristlose Entlassung nach einer Überwachung des Computers“

Quellen:

- Vernetzte Arbeitswelt – Chancen und Risiken. Die Zeit, 15.5.2016
- Vorsicht, der Chef surft mit. Süddeutsche Zeitung, 9.4.2016
- Wer zu viele private Mails verschickt, fliegt raus. Frankfurter Allgemeine, 15.1.2016
- Comment UBS flique ses employés. Le Matin, 4.7.2015
- Protectas ist zu neugierig. Beobachter, 26.6.2015
- Mobiles Arbeiten, aber sicher. Zürcher KMU, 25.6.2015
- Darf die Firma meinen Computer ausspionieren?, 20 Minuten, 24.6.2015
- Wie Firmen das Internetverhalten ihrer Mitarbeiter im Büro regulieren. Handelszeitung, 18.6.2015
- Werden wir bald ständig bei der Arbeit überwacht? 20 Minuten, 20.2.2015

OGD und BGÖ – 2 Instrumente für Transparenz in der Schweiz

Unter Open Government Data (OGD) versteht man die offene Zugänglichkeit von Behördendaten, um sie für die wissenschaftliche Forschung und Entwicklung, wirtschaftliches Wachstum und Transparenz in der Politik nutzen zu können. Während OGD ein Instrument der Aktivkommunikation darstellt, dessen Inhalte von den Behörden bestimmt werden, regelt das Öffentlichkeitsgesetz (BGÖ) den Zugang zu amtlichen Dokumenten der Bundesverwaltung auf Gesuch hin.

„Die Publikation und Bereitstellung von Behördendaten birgt ein grosses Potenzial, das bis dato in der Schweiz nur teilweise ausgeschöpft worden ist", schrieb der Bundesrat in seiner Open-Government-Data-Strategie 2014-2018. Er möchte deshalb möglichst viele Behördendaten frei zugänglich und wiederverwendbar machen. Die Datensätzen der öffentlichen Hand können der Entwicklung neuer Informationsdienstleistungen und wissenschaftlicher Erkenntnisse dienen. Ausserdem fördere die OGD-Strategie generell die Transparenz sowie die Kompetenz der politischen Akteure in ihrem sozialen Handeln, was einer erhöhten Akzeptanz und mehr Vertrauen in der Bevölkerung zuträglich ist. Positive Nebeneffekte sind eine durch Rückmeldungen der Nutzer verbesserte Datenqualität und eine erhöhte Effizienz der Behörden, die Daten einfacher interdisziplinär nutzen können.

Der EDÖB begrüsst die OGD-Strategie des Bundesrates und erachtet die seit Februar 2016 vom Bundesarchiv betriebene opendata.swiss-Plattform als weiteren wichtigen Schritt in den Transparenzbestrebungen des Bundes. Die im Februar 2016 lancierte Online-Plattform umfasst inzwischen über 1000 Datensätze von Bundesämtern, Kantonen, Städten und weiteren Organisationen.

10 Jahre Öffentlichkeitsgesetz

Auch das Öffentlichkeitsgesetz, das seit dem 1. Juli 2006 in Kraft ist, fördert die Transparenz in der Bundesverwaltung. Während OGD als Aktivinstrument den freien Zugang zu behördlichen Rohdatensätzen bezweckt, regelt das BGÖ den Zugang zu bestehenden amtlichen Dokumenten lediglich auf Gesuch hin. Es ist als Instrument der Passivinformation zu verstehen, was bedeutet, dass der Gesuchsteller Inhalt und Umfang der Daten, in die er Einblick haben will, selber bestimmen kann. Das BGÖ öffnet Einsichtswilligen Tür und Tor zu umfassenden Behördeninformationen.

In letzter Zeit sind Fälle bekannt geworden, wo überhöhte Gebühren den Zugang zu amtlichen Dokumenten verhindern sollten. Grenzen der Transparenz sind in gewissen Ausnahmefällen wie der inneren Sicherheit berechtigt. Sie dürfen aber den Grundgedanken des Öffentlichkeitsprinzips nicht unterlaufen. Eine parlamentarische Initiative verlangt nun weitgehende Gebührenbefreiung.

Aus Anlass des 10-jährigen Bestehens des Öffentlichkeitsprinzips in der Verwaltung findet am Freitag, 2. September 2016, in Bern eine öffentliche Tagung unter dem Titel „Wie transparent ist unsere Bundesverwaltung nach 10 Jahren Öffentlichkeitsgesetz?" mit Referaten und einer Podiumsdiskussion statt.

Information und Anmeldung auf unserer Website.

Weiterführende Informationen:

- Informationen zum BGÖ auf der Website des EDÖB www.derbeauftragte.ch / Öffentlichkeitsprinzip, insbesondere in unserem Merkblatt
- Die Open-Government-Data-Strategie 2014-2018 des Bundesrates ist auf dem Portal des Bundes publiziert

Quellen:

- Piquée au vif, Armasuisse jette 30'000 francs par la fenêtre. Le Matin Dimanche, 14.8.2016 (Armasuisse muss Agenda vorlegen. Der Bund, 15.8.2016)
- Plädoyer für Transparenz in der Verwaltung. NZZ, 28.6.2016
- Beim Nachrichtendienst gilt Transparenz mit Grenzen. NZZ, 19.5.2016
- Der Bund will eine „Open-Data-Kultur" fördern. NZZ,17.5.2016
- Le prix elevé de la transparence. Le Temps, 11.5.2016
- Kostenlose Transparenz. Sonntagszeitung, 8.5.2016
- Transparenz nur gegen Bares. Sonntagszeitung, 13.3.2016

In eigener Sache

Datenschutzaspekte beim Internetprotokoll IPv6

Das Internet ist heute die wichtigste Technologie zur Übermittlung jeder Art von Kommunikation geworden. Weil die IP-Adressen des gegenwärtig genutzten Internet Protokoll Version 4 (IPv4) in absehbarer Zeit erschöpft sind, wurde ein neues Internetprotokoll (IPv6) entwickelt. Im Vergleich zu IPv4 bietet IPv6 eine Reihe praktischer Vorteile, birgt aber auch gewisse Risiken für den Datenschutz und die Privatsphäre. Diese Risiken können mit geeigneten technischen und organisatorischen Massnahmen minimiert werden.

Lesen Sie dazu die ausführlichen Erläuterungen auf unserer Website.

Kurz beleuchtet

Monsterjagd mit dem Smartphone

Pokémon GO heisst die App, welche die halbe Welt in ihren Bann zieht und Datenschützern den Schweiss auf die Stirn treibt. Spieler wandeln mit ihrem Handy durch die Strassen, auf der Jagd nach den begehrten Monstern, die darauf warten, eingefangen zu werden. Der Spass am Spiel hat jedoch seinen Preis: die Nutzer gewähren der Applikation Zugriff auf ihre Standortdaten und können somit in Echtzeit geortet werden. Auch auf die Kamera greift die App für die Augmented-Reality-Funktion zu. Was der Anbieter mit diesen Daten macht und an wen er sie genau weitergibt, geht aus den langen Nutzungsbedingungen nur ungenügend hervor – eine Problematik, die auch zahlreiche andere Apps und Onlinedienste betrifft. Wir raten Nutzerinnen und Nutzern, genau hinzusehen, welche Berechtigungen eine App verlangt und abzuschätzen, ob diese erforderlich sind. Viele Anwendungen erfassen mehr Daten als für die Erbringung des Dienstes nötig wären. Wer dies nicht wünscht, sollte die Standardeinstellungen anpassen oder auf die Nutzung des Dienstes verzichten.

Tipps

Installation einer Videokamera in einem Mehrfamilienhaus

Zur Installation einer Videoüberwachungsanlage in einer privaten Liegenschaft braucht es keine Bewilligung, aber es müssen gewisse Regeln beachtet werden. Wer das Aufnahmefeld der Kamera betritt, muss beispielsweise mit einem Hinweisschild darüber informiert werden.

Geht dies aus den Umständen nicht bereits klar hervor, sollte auf dem Hinweisschild auch stehen, wo die Betroffenen Auskunft über die erhobenen Daten einholen können. Zudem sollte der Fokus der Kamera nur den absolut notwendigen Bereich erfassen, die Bilder sollten nicht länger als nötig aufbewahrt und vor unbefugtem Zugriff angemessen geschützt werden. Worauf Sie für einen datenschutzkonformen Betrieb einer Videoüberwachungsanlage alles achten müssen, finden Sie in unserem Merkblatt „Videoüberwachung durch private Personen“ detailliert beschrieben.

In einem Mehrfamilienhaus kann aber nicht ein einzelner Bewohner von sich aus eine Kamera in gemeinschaftlich genutzten Räumen installieren. Darüber müssen die Hausbewohner gemeinsam befinden, wobei ein Mehrheitsbeschluss nicht ausreicht. Wenn kein überwiegendes Interesse besteht, muss jeder Einzelne einverstanden sein.

Das Bundesgericht hält in seinem Urteil vom 29. März 2016 (BGE 4A_576/2015) fest, dass ein allgemeines Interesse des Hauseigentümers oder mehrerer Bewohner den Betrieb einer Videoüberwachungsanlage im Innern eines Mehrfamilienhauses nicht ohne weiteres rechtfertige. Ebenso wenig geht der Schutz der Privatsphäre (Art. 13 BV) der verfassungsrechtlichen Eigentumsgarantie (Art. 26 BV) oder dem Schutz auf körperliche Unversehrtheit (Art. 10 Abs. 2 BV) vor, so dass eine Videoüberwachung in gemeinschaftlichen Räumen ohne die Zustimmung sämtlicher Betroffener stets unzulässig wäre. Eine konkrete Interessenabwägung unter Einbezug sämtlicher Umstände des Einzelfalls ist deshalb unabdingbar. So kann eine Videoüberwachung im Eingangsbereich eines anonymen Wohnblocks, in dem gegebenenfalls gar ein Risiko von Übergriffen besteht, durchaus angezeigt und für alle betroffenen Personen zumutbar sein, während dies in einem kleineren Mehrfamilienhaus, wo sich die Nachbarn kennen, normalerweise nicht der Fall sein dürfte. Eine permanente Überwachung im Eingangsbereich eines Mehrfamilienhauses, die eine systematische Erhebung des Verhaltens von Bewohnern und Besuchern ermöglicht, stellt aber in jedem Fall einen erheblichen Eingriff in die Privatsphäre dar. Deshalb muss der Betrieb einer Videoüberwachungsanlage stets gerechtfertigt und verhältnismässig sein.

Weiterführende Informationen:

- Merkblatt „Videoüberwachung durch private Personen“ auf unserer Website
- Umfassende Informationen zu Videoüberwachung in weiteren Bereichen finden Sie ebenfalls auf unserer Website
- Bundesgerichtsentscheid (BGE 142 III 263) vom 29.3.2016

Quelle:

- Dürfen wir eine Videokamera installieren? Neue Luzerner Zeitung, 25.5.2016

Agenda

10 Jahre Öffentlichkeitsgesetz - Schweizerische Tagung zum Öffentlichkeitsprinzip in der Verwaltung:

Wie transparent ist unsere Bundesverwaltung nach 10 Jahren Öffentlichkeitsgesetz?

Freitag, 2. September 2016, Aula Progr, Waisenhausplatz 30, Bern

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

Impressum

August 2016

Übersetzungen: Schweizerische Bundeskanzlei, Sprachdienste

Dieser Newsletter ist auch auf Französisch und Italienisch erhältlich.

Der EDÖB im Internet: www.derbeauftragte.ch