01/2008

datum

Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Inhalt

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Editorial

Liebe Datenschutzinteressierte

Das Jahr 2008 hat für den EDÖB betriebsam begonnen. Während intern die Texte für den jährlichen Tätigkeitsbericht, mit dem der EDÖB gegenüber Bundesrat, Parlament und Öffentlichkeit Rechenschaft über seine Tätigkeit ablegt, erstellt, korrigiert und übersetzt werden, waren wir gleichzeitig mit der Organisation des 2. Europäischen Datenschutztages beschäftigt. Wie dieser Tag für die Sensibilisierung der Bevölkerung für Datenschutzgbelange genutzt wurde, lesen Sie im zweiten Artikel. Der erste Artikel nimmt ein vor allem unter jüngeren Generationen virulentes Thema auf: das Social Networking im Internet. Es ist mit beträchtlichen Risiken für die Privatsphäre verbunden, die mit den richtigen Massnahmen aber verringert werden können. In den Kurzrubriken behandeln wir unter anderem die datenschutzkonforme Suche im Internet und den Dauerbrenner Passwortsicherheit. Ich hoffe, Sie finden in den folgenden Seiten nützliche Informationen.

Eine gute Lektüre wünsche

Eliane Schmid
Redaktionsverantwortliche ◄

Themen

Social Networking: Ein Gesicht spricht Bände

Die Zahlen sprechen für sich: So genannte Social Networking Sites wie Facebook, MySpace oder StudiVZ (um nur einige zu nennen) verzeichnen monatliche Mitglieder-Zuwachsraten im zweistelligen Prozentbereich. Es wird kommuniziert, Gleichgesinnte werden kontaktiert, Bilder ausgetauscht, Freundschaften geschlossen, alte Schulkameraden gesucht, ehemalige Freunde oder ganz einfach Feinde hemmungslos diffamiert, Hasskampagnen geführt – alles schon da gewesen? Nicht ganz.

Gehen wir davon aus, der Mensch sei im Grunde ein soziales Wesen. Er will Kontakte mit anderen Menschen pflegen, sich austauschen können, nicht alleine sein. Was ältere Generationen noch in Turn- oder Wandervereinen, am Stammtisch, am Dorffest oder einfach im Freundes- und Familienkreis fanden, verlagert sich zunehmend ins Internet. So genannte Social Software erleichtert den Internetnutzerinnen und -nutzern das Hochladen von eigenen Inhalten ins Internet. Auf dieser Basis erst konnten sich Social Networking Sites (SNS), auf denen sich heute vor allem junge Leute «treffen» und Freundschaften schmieden, in den letzten Jahren entwickeln. Dabei geben viele von ihnen sehr persönliche Details preis, von Geburtsdatum und Adressen über Telefonnummern, kulturelle Vorlieben, politische oder religiöse Gesinnungen bis hin zu Fotos und Videoaufnahmen, die in Unzahl dem eigenen Profil beigefügt werden können. Aber genau diese Informationen, könnte hier eingewendet werden, wurden doch unter Teenage-Freundinnen und -Freunden schon immer ausgetauscht. Das mag stimmen. Nur hat der soziale Rahmen heute eine ganz andere Dimension.

Neue Grenzen …

Denn im Internet verschieben sich die Grenzen mehr und mehr. Reale geografische und zeitliche Distanzen sind aufgehoben, die Inhalte weltweit einsehbar. Dank Web 2.0 sind User zudem nicht länger nur Leserinnen und Leser von Inhalten, sondern eben auch Autorinnen und Autoren. Es zeigt sich, dass die Generation der «Internet-Eingeborenen» ein gewandeltes Verständnis von Privatsphäre

hat – viele Junge fühlen sich offensichtlich wohl damit, sogar intime Details ihres Lebens im Internet zu publizieren. Ihre Nutzerprofile sprechen Bände.

Das kann schwerwiegende Folgen haben. Provider solcher Social Networking Portale geben vor, sie brächten einfach die normale Kommunikation zwischen Freunden ins Internet. Die Wahrheit jedoch ist: Öffentlich einsehbare Informationen über Personen auf diesen Plattformen sind nicht mehr nur im Dorf, in der Talschaft oder im Stadtkreis im Umlauf – sondern weltweit. Wenn im Zusammenhang mit solchen Internetportalen also von community, von Gemeinschaft die Rede ist, so wird damit Vertrautheit vorgegaukelt und (bewusst?) verwischt, dass diese community in der Tat riesig gross und so gar nicht intim sein kann.

Eine direkte Folge davon ist, dass man als User den wahrscheinlich grössten Teil der «Freunde» nicht persönlich kennt und sich also auf die Aussagen in deren Profil verlassen muss. Klar: Man kann auch unter Augenkontakt angeschwindelt werden – jedoch dürfte es in der Realität bedeutend schwerer fallen, über längere Zeit ganze Teile der eigenen Identität zu verbergen und falsche Angaben über sich selbst zu machen. Im schriftlichen Kontakt hingegen ist es durchaus möglich, unter Vorspiegelung einer falschen Identität das Vertrauen einer Person zu erschleichen und so beispielsweise zu Informationen zu kommen, die einem das Gegenüber unter anderen Umständen vielleicht nie mitgeteilt hätte. Mit den SNS verändern sich Konzepte wie «Freundschaft» und «Vertraulichkeit» inhaltlich; Fälle, in denen solche «Freundschaften» in ausgeweitete Hass- oder Diffamierungskampagnen («cyberbullying», Rufmord) umschlugen, haben in den USA bereits zu Selbstmorden geführt.

Ein weiteres Problem ist die Löschung von Personendaten auf diesen SNS. Man kann zwar durchaus die Hauptseiten eines Profils löschen lassen, jedoch bleiben beispielsweise Kommentare, die ein User andernorts im Portal gemacht hat, bestehen. Zudem tun sich viele Provider solcher Plattformen offenbar schwer damit, Benutzerkonten auf Antrag wirklich zu löschen – oft werden sie lediglich deaktiviert. Generell gilt: Was im Internet einmal in Umlauf ist, wird es auch bleiben: Daten haben kein Verfallsdatum und es ist praktisch unmöglich, sie unwiderruflich zu entfernen, denn die Chance ist sehr gross, dass sie in privaten PCs oder im Cache von Suchmaschinen noch gespeichert sind – und also jederzeit wieder auftauchen können. Solcherart verliert man über die Daten, die man im Internet preisgibt, die Herrschaft.

… alte Verhaltensmuster …

Jugendliche haben zu allen Zeiten über die Stränge geschlagen. Weder Schikanen gegen einzelne Kameradinnen oder Kameraden auf dem Schulhof noch prononcierte politische Aufrufe, Alkohol- oder Drogenmissbrauch oder Teenie-Gespräche über

Als Ort «echter» Geselligkeit wohl schwer zu ersetzen: Das Lagerfeuer

Intimitäten sind Phänomene unserer Zeit. Werden solche Aktivitäten jedoch im Internet ausgeführt, gilt mehr denn je: Vorbei ist nicht unbedingt vorbei. Welchen Eindruck das Bild eines jugendlichen Zechgelages oder der Aufruf zu zivilem Ungehorsam auch Jahre später noch bei einem potenziellen Arbeitgeber hinterlassen kann, muss hier nicht weiter erörtert werden.

Ein weiterer wichtiger Aspekt ist die wirtschaftliche Seite der SNS-Medaille. Diese Dienste sind wohl zumeist gratis – aber nicht etwa, weil ein wohltätiger Philanthrop dahinter steckt, sondern weil Personendaten, wie wir an dieser Stelle nie müde werden zu betonen, im eigentlichen Sinne des Wortes kostbar sind. Das zeigt sich am sprunghaften Wertanstieg der einschlägigen Plattformen. Dabei geht es nicht nur um die vom Nutzer selber offenbarten Daten, sondern auch um seine Bewegungen auf der SNS, welche vom Provider minutiös gespeichert werden können: Welche Links klickt der Nutzer an, wie lange verweilt er auf welchen Informationen, etc. Zusammen ergeben diese Datenkategorien ausführliche Persönlichkeitsprofile, welche insbesondere für die Absender von personalisierter Werbung sehr interessant sind. Mehrere SNS-Anbieter sind in jüngster Vergangenheit denn auch unter dem Verdacht, solche Nutzerdaten und -profile verkauft zu haben, in die Schlagzeilen geraten. Damit dürfte eine schöne Stange Geld zu verdienen sein.

… und bekannte Schutzmechanismen

Social Networking Sites sind ein Phänomen des 21. Jahrhunderts. Entsprechend neu sind auch die Erfahrungen damit, und es ist davon auszugehen, dass weitere Risiken und Sicherheitslöcher auftauchen werden. Der Datenschutz steht dadurch immer wieder vor neuen Herausforderungen: War sein Hauptziel zunächst der Schutz der Privatsphäre der Bürgerinnen und Bürger vor staatlichen Zugriffen, so gefährden seit Jahren zunehmend wirtschaftliche Interessen die Privatsphäre des Einzelnen. Mit den SNS entsteht durch den Zugriff von Privatpersonen auf die Profile und Angaben anderer Nutzer nun eine neue Dimension, die in Identitätsdiebstahl, cyberbullying, cyberstalking und andere ähnliche Phänomene münden kann.

Ganz machtlos sind die User jedoch nicht: Als StudiVZ, eine deutsche Plattform für Studentinnen und Studenten, die AGB ändern wollte, um personalisierte Werbung zuzulassen, vereinigten sich zahlreiche User im Protest dagegen. Noch besser ist jedoch die Vorsorge:

- Seien Sie vorsichtig bei der Veröffentlichung Ihrer Personendaten (Name, Adresse, Telefonnummer) auf einer SNS. Benutzen Sie Pseudonyme.
- Fragen Sie sich vor der Veröffentlichung immer, ob Sie in einem Bewerbungsgespräch mit den entsprechenden Daten/Bildern konfrontiert werden möchten. Und zwar auch noch in zehn Jahren.
- Respektieren Sie die Privatsphäre Dritter, veröffentlichen Sie nicht deren Personendaten, also auch keine Bilder.
- Informieren Sie sich über die Anbieter

des Portals und wie die Privatsphäre der Nutzer gewährleistet wird. Hat der Dienst ein Datenschutz- oder Sicherheitsgütesiegel?

- Benutzen Sie verschiedene Logins und Passwörter für verschiedene Dienste.
- Behalten Sie die Internetaktivitäten Ihrer Kinder im Auge.

Weitere Tipps und nützliche Informationen finden Sie unter

- www.derbeauftragte.ch

und

- http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Quellen:

- European Network and Information Security Agency ENISA. Position Paper No. 1: Security issues and Recommendations for Online Social Networks. Editor: Giles Hogben. October 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
- Tages-Anzeiger vom 27.11.2007: Verhöhnt durch die Tyrannen des Internets.
- NZZ vom 16.11.2007: Erfolgversprechende Beziehungsnetze.
- Spiegel online vom 18. Dezember 2007: Studenten demonstrieren gegen das SchnüffelVZ. http://www.spiegel.de/netzwelt/web/0,1518,523906,00.html ◀

Der Datenschutz geht auf Sendung

Am 28. Januar 2008, dem 2. Europäischen Datenschutztag, nahmen sich Schweizer Radio DRS und Radio Suisse Romande in enger Zusammenarbeit mit dem EDÖB einige Datenschutzthemen vor. Während Hanspeter Thür, sein Stellvertreter Jean-Philippe Walter und weitere Fachleute in verschiedenen Sendungen zentrale Fragestellungen im Bereich des Schutzes der Privatsphäre herausarbeiteten, beantworteten zehn Expertinnen und Experten des EDÖB insgesamt über 200 Fragen aus der Bevölkerung.

Am Anfang war der Wissensmangel – Europas Bürgerinnen und Bürger weisen nämlich im Durchschnitt sehr wenige Kenntnisse über Datenschutz, Gefahren für die Privatsphäre und die eigenen Rechte auf. Dem will der Europarat mit dem jährlichen Datenschutztag entgegenwirken, und deshalb war für den EDÖB die Gelegenheit sehr günstig, mit zwei nationalen Radiosendern zusammenzuarbeiten, um ein möglichst breites Publikum ansprechen zu können. Eigens für diesen Tag wurde im Hintergrund in den Studios ein von EDÖB-Expertinnen und -Experten betreutes Beratungsangebot für die Zuhörerinnen und Zuhörer aufgezogen: eine Hotline bei DRS und ein Internet-Forum bei RSR. Von dieser Möglichkeit, sich direkt und unkompliziert Antworten und Ratschläge in Sachen Datenschutz zu holen, machten über 200 Zuhörerinnen und Zuhörer Gebrauch. Im Vordergrund gestalteten die Verantwortlichen von DRS und RSR spannende Sendungen und griffen sachlich, unaufgeregt und humorvoll aktuelle Datenschutzthemen auf, die sie mit zahlreichen Studiogästen – Fachleuten aus den Bereichen Datenschutz, Recht, Informatik, Telekommunikation oder Staatsschutz – besprachen. Einige zentrale Aussagen und Erkenntnisse sollen hier festgehalten werden.

Privatsphäre – was ist das eigentlich?

Denjenigen Zuhörerinnen und Zuhörern, die datenschützerische Anliegen bis anhin eher aus der Ferne vernommen hatten, lieferte Doris Slongo, Rechtsanwältin und Rechtsberaterin bei Schweizer Radio DRS, einen einfachen Einstieg: Die Privatsphäre ist der Teil der Persönlichkeit, den man für sich behalten oder nur mit einem kleinen Kreis Vertrauter teilen möchte – sicher aber nicht mit der Öffentlichkeit. Dabei handelt es sich beispielsweise um Angaben zur Gesundheit, zur finanziellen Situation oder zu religiösen und politischen Überzeugungen. Es ist dem Individuum freigestellt, wie offenherzig es mit solchen persönlichen Informationen umgeht. Jedoch sollte man im Hinterkopf behalten, dass Personendaten äusserst wertvoll sind. Professionelle Adresshändler verdienen nämlich viel Geld damit, nebst Adressen auch eine Vielzahl an Zusatzangaben zu den jeweiligen Personen zu verkaufen (siehe *datum* 1/2006). Die Käufer aus der Wirtschaft haben ein vitales Interesse daran, ihre Kunden möglichst genau zu kennen und exakt zu kategorisieren, um sie danach mit massgeschneiderten Angeboten beliefern und den eigenen Umsatz steigern zu können. So meinte der EDÖB Hanspeter Thür denn auch, das Interesse der Wirtschaft an den Daten sei nicht an sich anrüchig – stossend sei aber, dass nicht der Inhaber der Daten, also die betroffene Person, den Profit aus einem Verkauf der eigenen Daten ziehe, sondern ein Adresshändler.

Jugendsünden für die Ewigkeit

Damit verbunden entgleitet dem Individuum die Herrschaft über die eigenen Daten zunehmend, und dies nicht nur durch den Adresshandel, sondern auch und vor allem im Internet (siehe Artikel oben). Astrid Epiney, Rechtsprofessorin an der Universität Freiburg i. Ü., zog den Vergleich zu älteren Medien: Vor zwanzig Jahren konnte man ein Plakat mit einer bestimmten Botschaft entfernen, wenn es nicht mehr aktuell war. Stellt man heute Angaben ins Internet, ist das praktisch nicht mehr rückgängig zu machen. Die Internationalität des Mediums und der Anbieter sorgen für die globale Verbreitung von Informationen, und Löschungsbegehren sind meist aussichtslos. So kann es passieren, dass «Jugendsünden» politischer oder alkoholischer Natur zwar schon längst passé sind, im Internet aber immer noch «gegoogelt» werden können und sich so zu Stolpersteinen in der beruflichen Laufbahn entwickeln (siehe *datum* 1/2005). Ausnehmend heikel wäre unter diesem Blickwinkel gerade auch die Veröffentlichung von besonders sensiblen Personendaten – man stelle sich vor, ein Cracker verschaffte sich beispielsweise Zugang zu einer Gesundheitsdatenbank und stellte die Daten ins Internet; betroffene Personen könnten dadurch dauerhaft in grosse Schwierigkeiten geraten.

Hanspeter Thür und Claude-Marie Vadrot,

Journalist und Autor des Buches «La Grande Surveillance», gaben weiter zu bedenken, dass auch fehlerhafte Informationen, einmal im Netz verbreitet, kaum mehr aus der Welt zu schaffen sind. Unter diesem Blickwinkel dürfte sich auch die gegen den Datenschutz gerichtete, oft gehörte Aussage: «Ich habe nichts zu verbergen, also auch nichts zu befürchten!» erübrigen. Am Besten hält man es mit Solange Ghernaouti Hélie, Professorin an der Universität Lausanne und Spezialistin für cybersecurity und cybercrime. Sie hielt fest, man müsse nicht alles über sich enthüllen, bloss, weil man «nichts zu verbergen» habe. Wenn wir die Herrschaft über unsere Daten verlieren, merken wir früher oder später, dass nicht wir die Technologie beherrschen, sondern sie uns. ◄

Kurz beleuchtet

Suchmaschinen als Datenkraken – aber es geht auch anders

In den vergangenen Monaten wurden die umfassenden Datensammlungen verschiedener Suchmaschinenbetreiber und die Dauer der Speicherung der Daten von Datenschutzbeauftragten, Bürgerrechtsgruppen und in den Medien mehrfach kritisch beleuchtet. Nun hat das Datenschutzlabor der Carnegie Mellon University mit PrivacyFinder eine Suchmaschinenmaske entwickelt, die dem Datenschutz besser Rechnung trägt. PrivacyFinder ermöglicht dem Benutzer nebst der Auswahl der Suchmaschine (Google oder Yahoo!) auch die Angabe des gewünschten Datenschutzstandards (low, medium, high, custom). Entsprechend werden die Suchresultate aufgelistet, basierend auf der P3P-Technologie. Suchanfragen und IP-Adressen oder Nutzerkennungen werden übrigens nur eine Woche gespeichert. Die Reaktionszeit von PrivacyFinder ist etwas länger als die der herkömmlichen Suchmaschinen. Ihre Privatsphäre wird Ihnen die Geduld danken!

Quelle:

- Heise online, 26. März 2008 http://www.heise.de/newsticker/suche/ergebnis?rm=result;words=Privacy;q=privacy;url=/newsticker/meldung/105558/

Links:

- www.privacyfinder.org
- http://de.wikipedia.org/wiki/Platform_for_Privacy_Preferences
- http://en.wikipedia.org/wiki/P3P

Aus der Presse

Schwerwiegender falscher Verdacht

Gewissermassen im Anschluss an den Artikel über das Surfen mit WLAN im letzten *datum* sticht folgendes Geschehen ins Auge: Wieder kommt ein Unschuldiger in den Verdacht, Kinderpornografie aus dem Internet herunter geladen zu haben. Wieder fährt die Polizei ein, beschlagnahmt PC und Laptop – und wieder findet sie auf den Rechnern kein belastendes Material. Diesmal liegt der Haken allerdings nicht bei einem ungenügend gesicherten WLAN, kein Unbefugter hatte es zum Surfen benutzt. Der betroffene Professor nimmt sich einen Anwalt, und die Akteneinsicht mündet im Verdacht, der Fehler sei beim Internetprovider passiert. In der Tat räumt der Provider Tage später ein, bei der Zuordnung der IP-Adresse zu Name und Adresse des Kunden sei ein Fehler unterlaufen.

Der Professor hatte Glück im Unglück, denn Familie und Freunde hielten zu ihm. Das ist jedoch keineswegs selbstverständlich: Gerade angesichts solch schwerwiegender Anschuldigungen wankt die Verpflichtung zur Unschuldsvermutung nicht selten auch im sozialen Umfeld.

Quelle:

- heise online, News, 14.3.2008; http://www.heise.de/newsticker/IP-Verwechslung-fuehrt-zu-falschem-Kinderporno-Verdacht--/meldung/105094

Tipps

Passwortsicherheit

Die Passwortsicherheit ist ein Thema, über das schon viel Tinte vergossen worden ist. Dies wird auch in Zukunft so bleiben. Es besteht Einigkeit darüber, dass die «Robustheit» eines Passwortes von dessen Länge und der Kombination der verschiedenen Zeichen abhängt (Grossbuchstaben/Kleinbuchstaben/Zahlen/Sonderzeichen/Satzzeichen); umstrittener ist die Aufbewahrung der Passwörter.

Früher galt: Niemals ein Passwort aufschreiben, sondern einzig und allein im Kopf behalten, damit es nicht zu einfach entwendet werden kann. Diese Anforderung an die Sicherheit ist jedoch unvereinbar mit der Forderung nach der Robustheit eines Passwortes – zumal wir eine immer grössere Zahl komplizierter Passwörter auswendig lernen müssten.

Deshalb verwenden Benutzerinnen und Benutzer häufig ein und dasselbe Passwort für alle Anwendungen. Dies verringert die allgemeine Sicherheit ihrer Daten. Jesper Johanson (Microsoft) hat deshalb im Jahr 2005 vorgeschlagen, alle Passwörter auf ein Blatt Papier zu schreiben und dieses so gut wie möglich zu hüten. Dieser scheinbar alberne Vorschlag wurde sogar vom Sicherheitsexperten Bruce Schneier unterstützt. Er ist interessant, birgt aber das offenkundige Risiko, dass sich diese Passwortliste letztlich auf einem Postit am Bildschirmgehäuse oder unter der Mausmatte offenbart.

Aus diesem Grund raten wir dazu, eine Verschlüsselungssoftware für die Verwaltung der persönlichen Passwörter zu verwenden. Solche Programme sind in der Regel gratis (Password Corral, Password Safe, KeePass); sie erlauben es, die Gesamtheit der eigenen Passwörter zu schützen und diese in Untergruppen einzuteilen. Ein «Master-Passwort» – das als einziges auswendig gelernt werden muss – verschafft den Zugang zu den verschiedenen Passwörtern. Eine solche Verschlüsselungssoftware kann ohne weiteres auf einem Firmenrechner, einem privaten Computer, einem PDA oder einem Mobiltelefon installiert werden.

- http://www.cygnusproductions.com/freeware/pc.asp
- http://passwordsafe.sourceforge.net/
- http://keepass.info/

In eigener Sache

Revision des DSG

Am 1. Januar 2008 trat das revidierte Datenschutzgesetz in Kraft. Wesentliche Änderungen betreffen die erhöhte Transparenz bei der Bearbeitung von Personendaten, die Erleichterung der Meldepflicht bei der Übermittlung von Daten ins Ausland und die Möglichkeit der Zertifizierung von Datenverarbeitungsprodukten und -systemen.

Neu muss eine Datenbearbeitung und deren Zweck für die betroffene Person erkennbar sein – also entweder aus den Umständen ersichtlich oder explizit erwähnt werden. Auch über die Weitergabe an Dritte muss die betroffene Person in Kenntnis gesetzt werden, wenn diese Weitergabe nicht offensichtlich ist. Zudem muss der Datenbearbeiter, wenn er besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft, die Betroffenen in jedem Fall informieren.

Im Fall der Übermittlung von Daten ins Ausland betont das revidierte Gesetz die Verantwortung des Datenbearbeiters – neu muss die Übermittlung nicht immer dem EDÖB gemeldet werden. Nach wie vor muss aber im Zielland ein «angemessener Schutz» für die Daten gewährleistet sein. Ist er das nicht, ist die Bekanntgabe der Daten nur unter ganz bestimmten Voraussetzungen, die in Art. 6 Abs. 2 aufgelistet sind, zulässig.

Neu schafft das Gesetz die Möglichkeit einer Zertifizierung von Produkten und Verfahren im Zusammenhang mit der Bearbeitung von Personendaten. Akkreditierte unabhängige Zertifizierungsstellen sollen dieses Datenschutz-Label erteilen und damit zur Einhaltung von Normen und einer hohen Datenschutz-Qualität beitragen.

Weitere detaillierte Informationen finden Sie auf unserer Website:

- http://www.edoeb.admin.ch/themen/00794/00819/01086/index.html?lang=de

Neuerscheinung

Brunner, Stephan C. und Mader, Luzius. Öffentlichkeitsgesetz – Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 17. Dezember 2004 (BGÖ). Stämpfli Verlag AG, Bern 2008.

Agenda 2008

30. Juni	Jahresmedienkonferenz EDÖB, Veröffentlichung des 15. Tätigkeitsberichts
Oktober	*datum* 02/2008