Republik Österreich
Datenschutz behörde

NEWSLETTER 1/2016

# 2 Jahre Datenschutzbehörde, 1 Jahr Newsletter!

Die Publikation des ersten Newsletters im Jahr 2016 ist ein geeigneter Zeitpunkt, um innezuhalten und über die vergangenen 2 Jahre Resümée zu ziehen. Die Datenschutzbehörde nahm am 1. Jänner 2014 ihren Dienstbetrieb auf und löste die Datenschutzkommission ab. In diesen zwei Jahren hat sich im Bereich des Datenschutzes vieles getan. Der EuGH postulierte das Recht auf Vergessen, hob die Vorratsdatenspeicherrichtlinie auf und erklärte die Entscheidung der Kommission zur Datensicherheit in den USA – die sogenannte Safe Harbour Entscheidung – am 6. Oktober 2015 schlicht für ungültig. Diese – datenschutzrechtlich bahnbrechende – Entscheidung ist dem Engagement eines Österreichers – Maximilian Schrems – zu verdanken, der sich nicht damit zufrieden geben wollte, dass Facebook ihm letztlich zwar Auskunft über die Verwendung seiner Daten gegeben hat, aber die systematische Datenabschöpfung durch US Behörden, nicht verhindert hat (nicht verhindern konnte (?)).

Auch auf nationaler Ebene ist viel passiert; gleich ob dies das Erkenntnis des Verfassungsgerichtshofs aus dem Juni 2014 ist, mit dem die österreichischen Bestimmungen zur Vorratsdatenspeicherung für verfassungswidrig erklärt wurden, oder das Erkenntnis vom November 2015, mit dem § 28 Abs. 2 DSG 2000 (Widerspruchsrecht) als verfassungswidrig aufgehoben wurde. Anders als der EuGH im Fall Schrems, gewährt der VfGH in Hinblick auf § 28 Abs. 2 eine „Reparaturfrist“ bis Ende 2016 für den Gesetzgeber.

In diesem internationalen und nationalen Gewässer haben wir uns die letzten beiden Jahre bewegt. Darüber hinaus ist es innerbehördlich gelungen die Rückstände im Datenverarbeitungsregister abzubauen und sicherzustellen, dass (vorabkontrollpflichtige) Anträge rasch behandelt werden können. Auch im Bereich der Beschwerdeverfahren konnte eine deutliche Senkung der Bearbeitungsdauer erreicht werden. Zudem nahm die DSB verstärkt zu Gesetzesvorhaben Stellung.

Die Mitarbeiterinnen und Mitarbeiter der Behörde führen jährlich amtswegige Schwerpunktverfahren durch. In diesen Verfahren wird die Einhaltung datenschutzrechtlicher Vorschriften in bestimmten Sektoren geprüft. 2014 wurde der Sektor der Kreditauskunfteien geprüft, 2015 lag der Schwerpunkt auf Krankenanstalten.

Darüber hinaus ist die DSB in ihrer Funktion als Stammzahlenregisterbehörde bei der Errichtung des Kontenregisters gefordert und wird auch bei der Einrichtung des Spendenregisters ihren Beitrag zu leisten haben.

Ein nationaler und internationaler Themenschwerpunkt der nächsten Jahre wird die Umsetzung der europäischen Datenschutz-Grundverordnung und der Datenschutz-Richtlinie für den Bereich Justiz und Inneres sein. Auf die DSB werden viele Neuerungen zukommen, wie etwa verstärkte Beratungsleistungen, Zertifizierung von Datenschutzsiegeln und (datenschutzrechtliche) Verhaltensrichtlinien in und für Unternehmen zu „approbieren“, sowie die Führung von Verwaltungsstrafverfahren. Die internationale Zusammenarbeit wird noch wichtiger als bisher werden und die Mitarbeiterinnen und Mitarbeiter werden ihre Fähigkeiten und Fertigkeiten im Bereich des Europäischen Datenschutzausschusses unter Beweis zu stellen haben. Eine genaue Analyse der Bestimmungen der Verordnung und der Richtlinie nach deren Beschlussfassung *) wird zeigen, welche Mittel die DSB zur Wahrnehmung dieser zusätzlichen Aufgaben benötigen wird

und ob andere Aufgabenbereiche hintangestellt werden können.

Seit einem Jahr wird nun der vierteljährlich erscheinende Newsletter versendet. Die positiven Rückmeldungen zeigen, dass es der DSB gelungen ist, ein ansprechendes Medium zu schaffen, das informativ und interessant ist. Zielsetzung war und ist, ein möglichst breites Publikum anzusprechen, da Datenschutz alle betrifft und nicht nur einige wenige „Wissende und Eingeweihte". Die neue Rubrik „Teens and Kids" verdeutlicht dies. An dieser Stelle sei Dank und Anerkennung all jenen Mitarbeiterinnen und Mitarbeitern der DSB ausgesprochen, die für die inhaltliche und optische Gestaltung des Newsletters verantwortlich sind und diese Aufgabe mit großem Engagement erfüllen.

Die DSB wünscht allen Leserinnen und Lesern des Newsletters alles Gute für das Jahr 2016 und viel Freude beim Lesen.

*) Textfassung vom 17. Dezember 2015

## Im Fokus

Mag. Michael Suda

### BVwG bestätigt Rechtsansicht der DSB zum Auskunftsrecht

Das Bundesverwaltungsgericht (BVwG) hat im Erkenntnis vom 17.11.2015, W214 2014069-1/15E (Abweisung der Bescheidbeschwerde, ordentliche Revision an den VwGH nicht zugelassen), einen Bescheid der DSB zum Auskunftsrecht bestätigt. Es besteht kein Recht, nach erfolgter Löschung von Daten (faktische Unmöglichkeit der Auskunftserteilung) die bescheidmäßige Feststellung von der DSB zu erlangen, dass vor erfolgter Löschung eine Verletzung im Recht auf Auskunftserteilung gegeben war. Das Beschwerdeverfahren gemäß § 31 Abs.1 DSG 2000 dient der Durchsetzung des Auskunftsrechts im Sinne einer Auskunftserteilung, nicht jedoch der Feststellung möglicher vergangener und nicht mehr beseitigbarer Rechtsverletzungen.

Anlassfall war das durch den Bescheid vom 1.10.2014, DSB-D122.020/0012-DSB/2014 (RIS), abgeschlossene Beschwerdeverfahren wegen Auskunftserteilung über die von einem Telekommunikationsunternehmen gespeicherten Vorratsdaten. Diese Daten waren nach dem 1. Juli 2014 (Wirksamwerden der Aufhebung der Bestimmungen über die Vorratsdatenspeicherung durch Erkenntnis des VfGH vom 27. Juni 2014, G 47/2012 u.a.) wegen Wegfalls der gesetzlichen Grundlage für die Speicherung gelöscht worden.

### VfGH hebt § 28 Abs. 2 DSG 2000 auf

Der Verfassungsgerichtshof (VfGH) hat mit Erkenntnis vom 8. Oktober 2015, G 264/2015, § 28 Abs. 2 DSG 2000 als verfassungswidrig aufgehoben. Die Aufhebung tritt mit Ablauf des 31. Dezember 2016 in Kraft. Sollte bis dahin keine gesetzliche Neuregelung getroffen worden sein, muss ab 1. Jänner 2017 jeder Widerspruch gegen die Verwendung personenbezogener Daten gegenüber dem Auftraggeber begründet werden, auch im Fall einer nicht gesetzlich angeordneten Aufnahme von Daten in eine öffentlich zugängliche Datenanwendung.

Anlassfall war die Klage eines niedergelassenen Arztes auf Löschung seiner berufsbezogenen Daten aus dem Datenbankinhalt einer von einem Privatunternehmen betriebenen Website zur Ärztesuche. Die berufsbezogenen Daten waren rechtmäßig ermittelt worden (über ein öffentlich zugängliches Verzeichnis der Ärztekammer).

Nach Ansicht des VfGH war der durch § 28 Abs. 2 DSG 2000 normierte Eingriff in das Recht auf Meinungsäußerungs- und Informationsfreiheit gemäß Art 10 Abs. 1 EMRK unverhältnismäßig.

Kommentar: Das Höchstgericht hatte über eine Grundrechtekollision (§ 1 Abs. 1 DSG 2000 contra Art 10 Abs. 1 EMRK) zu entscheiden und hat dem Recht auf Informationsfreiheit hier den Vorrang eingeräumt. Wenn man das Erkenntnis genau liest, kommt man zu dem Schluss, dass den Gerichtshof vor allem die Besorgnis motiviert hat, § 28 Abs. 2 DSG 2000 könnte dazu verwendet werden, Online-Meinungsäußerungen (z.B. in privaten Blogs oder Diskussionsforen), die sich auf eine bestimmte Person beziehen, durch die Ausübung des begründungsfreien Widerspruchsrechts nach Belieben zu unterdrücken. Bei publizistischen Datenanwendungen, für die nicht ein Medienunternehmen als datenschutzrechtlicher Auftraggeber haftet (letztere sind durch das „Medienprivileg" des § 48 Abs. 1 DSG 2000 geschützt), wäre dies gemäß dem Wortlaut der aufgehobenen Bestimmung tatsächlich möglich gewesen. Durch die Entscheidung des VfGH soll sichergestellt werden, dass dem datenschutzrechtlichen Auftraggeber im Einzelfall stets ein Spielraum zur Vornahme einer Interessenabwägung bleibt.

### VfGH erweitert Befugnisse der Versicherungen

Der Verfassungsgerichtshof (VfGH) hat im Erkenntnis vom 8. Oktober 2015, G 20/2015, G 281/2015, die Wortfolgen „und Versicherern" und „oder Versicherungsnehmern oder Versicherungswerbern" in § 67 Gentechnikgesetz (GTG) sowie den letzten Satz in § 11a Abs. 1 Versicherungsvertragsgesetz (VersVG) als verfassungswidrig aufgehoben. Die Aufhebung tritt mit Ablauf des 31. Dezember 2016 in Kraft. Die Entscheidung erging in einem Verfahren betreffend einen

Individualantrag auf Gesetzesprüfung (Art 140 Abs. 1 B-VG) mehrerer Versicherungsunternehmen.

Damit ist es Versicherungen ab 1. Jänner 2017, vorbehaltlich einer anders lautenden gesetzlichen Nachfolgeregelung, nicht mehr absolut verboten, Ergebnisse von Genanalysen von Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten, die Verarbeitung entsprechender Daten eingeschlossen. Zulässig wird damit die Verwendung von Daten genetischer Analysen des Typs 1 (§ 65 Abs. 1 Z 1 GTG; Feststellung einer bestehenden Erkrankung). Unzulässig bleibt die Verwendung von Daten genetischer Analysen der Typen 2 bis 4 (§ 65 Abs. 1 Z 2 bis 4, insbesondere die Feststellung einer Prädisposition für eine Krankheit) für Zwecke der Risikoabschätzung durch ein Versicherungsunternehmen.

Nach dem Erkenntnis des VfGH ist die durch das ausnahmslose Verbot des § 67 GTG iVm § 11a VersVG bewirkte Ungleichbehandlung von Ergebnissen konventioneller Untersuchungen und genetischer Analysen des Typs 1 iSd § 65 Abs. 1 Z 1 GTG sachlich nicht gerechtfertigt. Die Bestimmungen wurden daher wegen Eingriffs in das Grundrecht auf Gleichheit vor dem Gesetz aufgehoben.

## Ausgewählte Entscheidungen der Gerichte

### Entscheidung EuGH Rs C-362/14

**Ungültigerklärung der Safe Harbor-Entscheidung der Europäischen Kommission durch den EuGH**

Der Europäische Gerichtshof hat am 6. Oktober 2015 die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Auf Grundlage der ursprünglichen Safe-Harbor Entscheidung war der Großteil des Datenverkehrs zwischen den Unternehmen in Mitgliedstaaten der Europäischen Union und den USA genehmigungsfrei gewesen. Im Gegensatz zu anderen Angemessenheitsentscheidungen der Europäischen Kommission galt diese Entscheidung nur für Unternehmen in den USA, die sich selbst zur Einhaltung bestimmter Datenschutzregeln verpflichtet hatten, nicht für das ganze Land.

Während das Urteil für den Datenverkehr zwischen Privatpersonen keine Auswirkungen hat, sind Datentransfers an Unternehmen in den USA, die bisher ausschließlich auf Grund von Safe Harbor genehmigungsfrei waren, auf dieser Grundlage nicht mehr geboten.

Falls personenbezogene Daten an Empfänger in den USA transferiert werden, die Mitglied im Safe Harbor sind, besteht die Möglichkeit, die Daten aus den USA „zurückzuholen“ und lokal bzw. auf einem anderen Server zu verarbeiten. Das heißt, entweder auf einem unternehmenseigenen Server, einem Server in einem EU-Mitgliedstaat oder einem anderen Staat mit angemessenem Datenschutzniveau. Dies sind alle Länder des Europäischen Wirtschaftsraums (EWR) und einige andere Länder, die in der Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV) Erwähnung finden.

Auch sehen die §§ 12 und 13 Datenschutzgesetz 2000 zahlreiche Alternativen vor. Dazu gehören unter anderem

- die Erfüllung von eindeutig im Interesse des Betroffenen abgeschlossenen Verträgen (§ 12 Abs. 3 Z 6 DSG 2000), z.B. Kaufverträge, bei denen der Geschäftspartner seinen Sitz in den USA hat
- die Weitergabe der personenbezogenen Daten mit Zustimmung des Betroffenen (§ 12 Abs. 3 Z 5 DSG 2000),
- die Weitergabe von veröffentlichten Daten (§ 12 Abs. 3 Z 1 DSG 2000),
- wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden (§ 12 Abs. 3 Z 7 DSG 2000),
- wenn die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6 DSG 2000) oder Musterverordnung (§ 19 Abs. 2 DSG 2000) ausdrücklich angeführt ist (§ 12 Abs. 3 Z 7 DSG 2000).

Die Europäische Kommission hat in ihrer offiziellen Stellungnahme zur Safe-Harbor-Entscheidung vom 6. Oktober 2015 unter anderem festgehalten, dass ein Transfer personenbezogener Daten in die USA auch in Zukunft auf Mechanismen wie Standardvertragsklauseln (2001/497/EG, 2004/915/EG oder 2010/87/EG) und Binding Corporate Rules (Verbindliche unternehmensinterne Vorschriften) gestützt werden kann. Die Datenschutzbehörde behält sich (diesbezüglich) im Rahmen des Genehmigungsverfahrens aber die Beurteilung des im Empfängerstaat geltenden angemessenen Datenschutzniveaus gemäß § 13 Abs. 2 DSG 2000 im Einzelfall vor.

Stellt sich ein Datenverkehr mit den USA als genehmigungspflichtig heraus, ist ein entsprechender Antrag an die Datenschutzbehörde zu stellen, die darüber bescheidmäßig innerhalb von maximal 6 Monaten abzusprechen hat. Dem Antrag sind die Begründung für die Genehmigungspflicht sowie die erforderlichen Unterlagen (Angabe, ob die Meldepflicht beim Datenverarbeitungsregister erfüllt wurde, vertragliche Zusicherung des Empfängers in Form von Standardvertragsklauseln, dass schutzwürdige Geheimhaltungsinteressen vom Empfänger gewahrt werden bzw. einseitige Zusagen im Zusammenhang mit Binding Corporate Rules) beizulegen. Eine solche Eingabe ist gebührenpflichtig.

Entscheidung C-362/14 im Volltext unter:

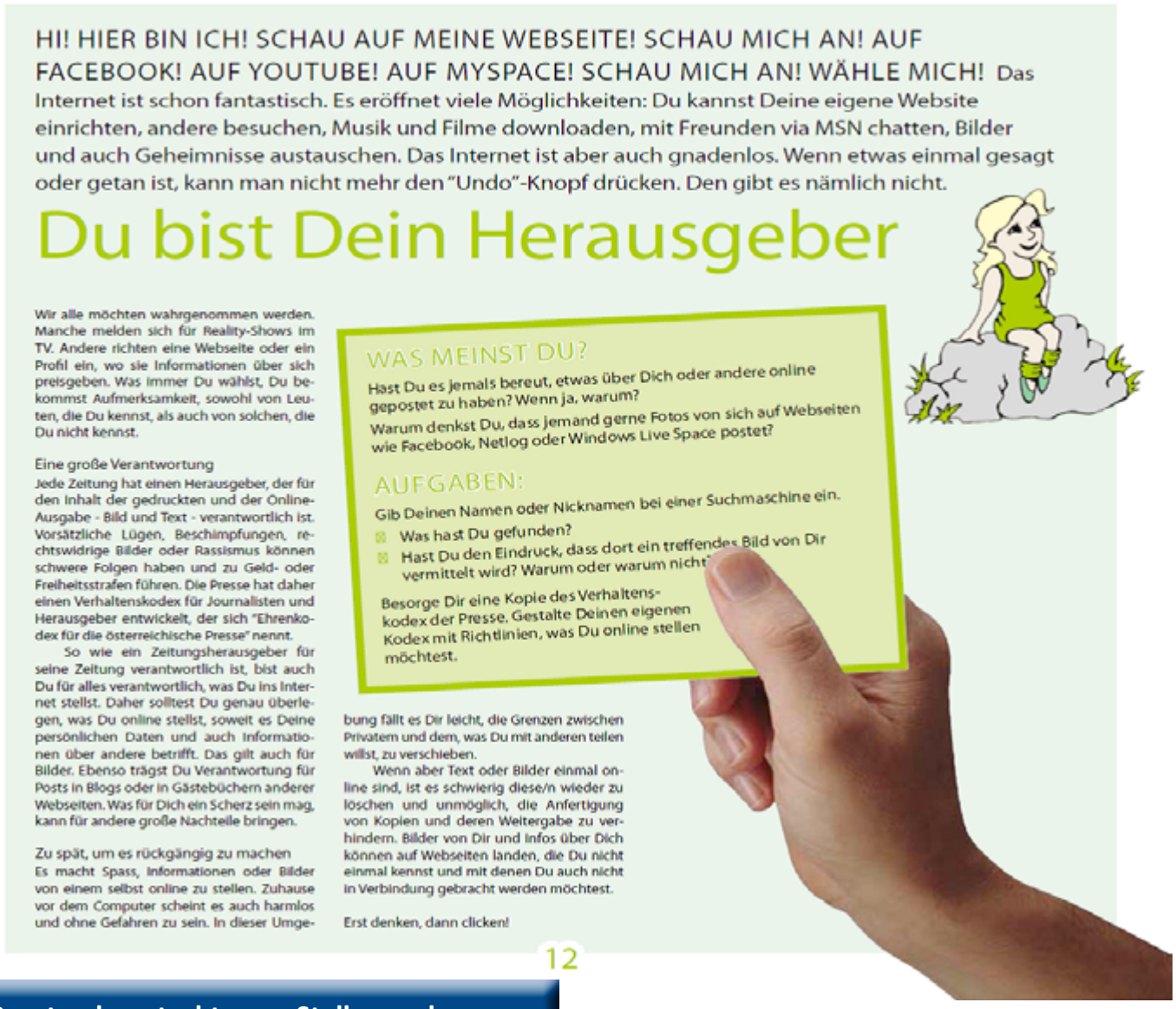
- http://www.dsb.gv.at/site/6218/default.aspx

## Teens & Kids

**Ein unverhüllter Trend unter Jugendlichen:**
„Sexting“: das Versenden von Nackt-Selfies.

Einmal verschickt, kann sich die Kontrolle über eigene freizügige Fotoaufnahmen schnell verlieren. So besteht die Gefahr, dass die intimen Bilder in sozialen Netzwerken landen. Durch fremde Personen können sie in der Folge für eigene oder fremde Zwecke in der Öffentlichkeit (zB.: Erotikseiten) verwendet werden und es besteht durchaus die Gefahr, dass diese Bilder Jahre später auch im Rahmen der Jobsuche auftauchen und Folgen nach sich ziehen. Die Löschung solcher Nacktfotos im Internet gestaltet sich sehr schwierig.Darüber hinaus ist gemäß § 207a StGB die Weitergabe, sowie unter gewissen Umständen, auch der Besitz von Nacktfotos bei Jugendlichen unter 18 Jahren strafbar.

Weitere Informationen und Tipps auf www.rataufdraht.orf.at, www.saferinternet.at und in der Broschüre „Du bestimmst - Datenschutz-Fakten und Gefahren“ der DSB auf www.dsb.gv.at:



HI! HIER BIN ICH! SCHAU AUF MEINE WEBSEITE! SCHAU MICH AN! AUF FACEBOOK! AUF YOUTUBE! AUF MYSPACE! SCHAU MICH AN! WÄHLE MICH! Das Internet ist schon fantastisch. Es eröffnet viele Möglichkeiten: Du kannst Deine eigene Website einrichten, andere besuchen, Musik und Filme downloaden, mit Freunden via MSN chatten, Bilder und auch Geheimnisse austauschen. Das Internet ist aber auch gnadenlos. Wenn etwas einmal gesagt oder getan ist, kann man nicht mehr den "Undo"-Knopf drücken. Den gibt es nämlich nicht.

Du bist Dein Herausgeber

Wir alle möchten wahrgenommen werden. Manche melden sich für Reality-Shows im TV. Andere richten eine Webseite oder ein Profil ein, wo sie Informationen über sich preisgeben. Was immer Du wählst, Du bekommst Aufmerksamkeit, sowohl von Leuten, die Du kennst, als auch von solchen, die Du nicht kennst.

Eine große Verantwortung

Jede Zeitung hat einen Herausgeber, der für den Inhalt der gedruckten und der Online-Ausgabe - Bild und Text - verantwortlich ist. Vorsätzliche Lügen, Beschimpfungen, rechtswidrige Bilder oder Rassismus können schwere Folgen haben und zu Geld- oder Freiheitsstrafen führen. Die Presse hat daher einen Verhaltenskodex für Journalisten und Herausgeber entwickelt, der sich "Ehrenkodex für die österreichische Presse" nennt.

So wie ein Zeitungsherausgeber für seine Zeitung verantwortlich ist, bist auch Du für alles verantwortlich, was Du ins Internet stellst. Daher solltest Du genau überlegen, was Du online stellst, soweit es Deine persönlichen Daten und auch Informationen über andere betrifft. Das gilt auch für Bilder. Ebenso trägst Du Verantwortung für Posts in Blogs oder in Gästebüchern anderer Webseiten. Was für Dich ein Scherz sein mag, kann für andere große Nachteile bringen.

Zu spät, um es rückgängig zu machen

Es macht Spass, Informationen oder Bilder von einem selbst online zu stellen. Zuhause vor dem Computer scheint es auch harmlos und ohne Gefahren zu sein. In dieser Umgebung fällt es Dir leicht, die Grenzen zwischen Privatem und dem, was Du mit anderen teilen willst, zu verschieben.

Wenn aber Text oder Bilder einmal online sind, ist es schwierig diese/n wieder zu löschen und unmöglich, die Anfertigung von Kopien und deren Weitergabe zu verhindern. Bilder von Dir und Infos über Dich können auf Webseiten landen, die Du nicht einmal kennst und mit denen Du auch nicht in Verbindung gebracht werden möchtest.

Erst denken, dann clicken!

WAS MEINST DU?

Hast Du es jemals bereut, etwas über Dich oder andere online gepostet zu haben? Wenn ja, warum?

Warum denkst Du, dass jemand gerne Fotos von sich auf Webseiten wie Facebook, Netlog oder Windows Live Space postet?

AUFGABEN:

Gib Deinen Namen oder Nicknamen bei einer Suchmaschine ein.

- Was hast Du gefunden?
- Hast Du den Eindruck, dass dort ein treffendes Bild von Dir vermittelt wird? Warum oder warum nicht?

Besorge Dir eine Kopie des Verhaltenskodex der Presse. Gestalte Deinen eigenen Kodex mit Richtlinien, was Du online stellen möchtest.

12

## Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Gerichtsgebühren-Novelle 2015
- Informationsfreiheitsgesetz

**Weblink:**
- Parlament aktiv: alle Stellungnahmen

**Impressum:**
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Hohenstaufengasse 3, 1010 Wien, E-Mail: dsb@dsb.gv.at, Web: http://www.dsb.gv.at

**Offenlegung gemäß § 25 Mediengesetz:**
Der Newsletter der DSB ist ein wiederkehrendes elektronisches Medium (§ 1 Abs. 1 Z 5a lit. c MedienG); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: http://www.dsb.gv.at/impressum.