

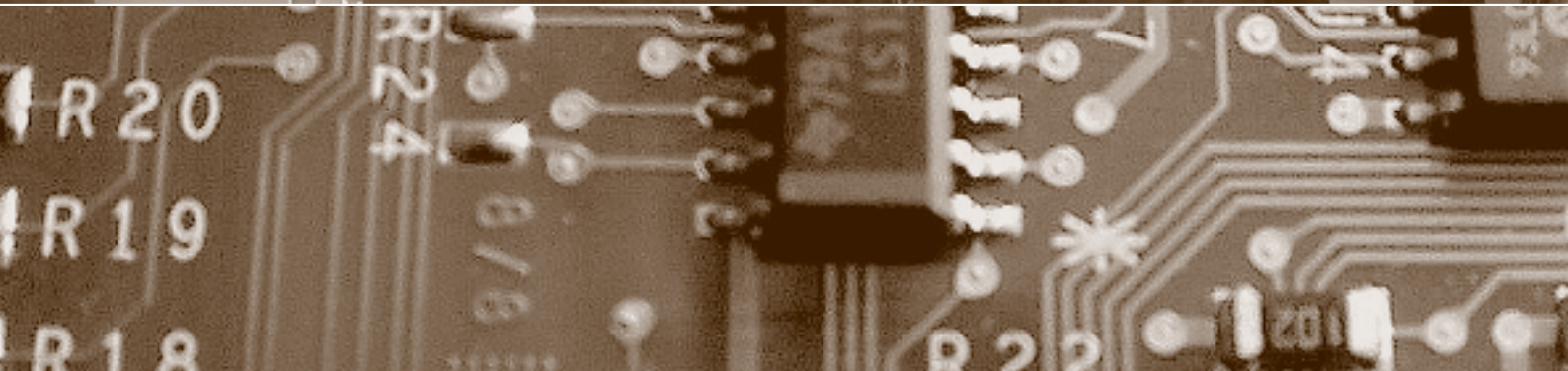
Schwerpunkt:

Faktor Mensch

fokus: Informationssicherheitskultur

fokus: Rechtliche Stolpersteine bei «BYOD»

report: Datenschutzaufsicht über Spitäler



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

fokus

Schwerpunkt:

Faktor Mensch

auftakt

Mitmachgesellschaft – oder Partizipation?

von Otfried Jarren Seite 145

Den Faktor Mensch miteinbeziehen

von Bernhard M. Hämmerli Seite 148

Informationssicherheitskultur

von Thomas Schlienger Seite 150

Loyalität im «Nomad Age»

von Marcus Beyer Seite 154

Rechtliche Stolpersteine bei «BYOD»

von Mark A. Reutter/
Samuel Klaus Seite 160

Vom Büro zur neuen Arbeitswelt

von Monika Josi Seite 166

Der Heilige Gral der Informationssicherheit

von Matthew Smith/Marian Harbach/
Sascha Fahl Seite 170

Nur befähigte, verantwortungsbewusste und loyale Mitarbeitende sind in der Lage, sich sicher zu verhalten. Mit einem gezielten Prozess kann erfolgreich eine geeignete Informationssicherheitskultur aufgebaut werden, die das ermöglicht. Wie kann eine solche Informationssicherheitskultur gemessen, geplant und gesteuert werden?

Informationssicherheitskultur

Bei den Mitarbeitenden ein «Grundrauschen» zum Thema Informationssicherheit zu erreichen, ist keine grosse Herausforderung mehr. Doch welche Rolle kommt dabei den Führungskräften zu? Loyalität wird zum Motor für eine aktive und gelebte Sicherheitskultur.

Loyalität im «Nomad Age»

«Bring Your Own Device» wirft verschiedene arbeits- und datenschutzrechtliche Fragen auf. Arbeitgeber, welche die Nutzung privater Geräte wie Laptops oder Smartphones zulassen, sollten vorgängig diese Fragen klar regeln.

Rechtliche Stolpersteine bei «BYOD»

IT-Sicherheits- und Privatsphärenmechanismen sind nur effektiv, wenn sie vom Menschen verstanden und korrekt angewendet werden. Der Mensch muss deshalb als integraler Teil eines soziotechnischen Systems begriffen und in die Entwicklung von anwenderfreundlichen Sicherheitsmechanismen einbezogen werden.

Usable Security

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtchenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com



Datenschutzaufsicht über Spitäler

Seit Januar 2012 erfüllen Spitäler im Bereich der Grundversicherung öffentliche Versorgungsaufgaben im Auftrag der Kantone. Auch die Privatspitäler, die im Rahmen kantonaler Leistungsaufträge tätig sind, unterstehen deshalb dem kantonalen Datenschutzrecht und folglich der Aufsicht durch die kantonalen Datenschutzbeauftragten.

Neue Spitalfinanzierung

Datenschutzaufsicht über Spitäler

von Bernhard Rütsche Seite 176

agenda

Seite 181

Forschung

Erkennung neuer Schadprogramme

von Jan Gassen/

Elmar Gerhards-Padilla

Seite 182

transfer

Cloud Computing:

Chancen und Risiken

von Roland Portmann

Seite 186

Erkennung neuer Schadprogramme

Computersysteme sehen sich immer neuen Cyber-Bedrohungen ausgesetzt. Bevor Computersysteme jedoch effizient vor solchen Bedrohungen geschützt werden können, müssen diese zunächst erkannt und analysiert werden. Um dies zu erreichen, leisten sogenannte Honeypots einen wertvollen Beitrag.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die neue Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzzsene.



Privatim

Aus den Datenschutzbehörden

von Sandra Husi-Stämpfli

Seite 188

privatim

Resolution

verabschiedet am Herbstplenium von

privatim

Seite 191

Sicherheitslücke

Sie suchen die Lösung, um die letzte Sicherheitslücke zu beseitigen? Unser Cartoonist stellt sie vor.

schlussstakt

Man muss Menschen mögen

von Beat Rudin

Seite 192

cartoon

von Reto Fontana



privatim

Aus den Daten- schutzbehörden



Sandra Husi-
Stämpfli, Dr. iur.,
Stv. Datenschutz-
beauftragte des
Kantons Basel-
Stadt, Basel
sandra.husi@dsb.
bs.ch

Ein spannendes Jahr neigt sich dem Ende zu. An dieser Stelle ein herzliches Dankeschön an all jene, welche uns mit Neuigkeiten aus den Datenschutzbehörden versorgt haben. Wir sind davon überzeugt, dass auch das Jahr 2013 interessante Themen mit sich bringen wird.

SIS: Was lange währt ...?

Die EU-Kommission teilte mit, dass die zweite Generation des Schengener Informationssystems (SIS II) nun endlich auf dem richtigen Weg zu sein scheint. Der zweite Meilensteintest ist erfolgreich verlaufen, und man gehe davon aus, dass das SIS II im ersten Quartal 2013 in Betrieb genommen werden könne. Allzu frühe Euphorie sollte an dieser Stelle jedoch vermieden werden: Noch stehen weitere Tests an, und die Leidensgeschichte des SIS II hat gezeigt, dass grosser Durchhaltewille gefordert ist, bis das System endlich «offiziell» läuft.

Bildungsraum Nordwestschweiz

Um die Synergien des Bildungsraums Nordwestschweiz zu nutzen, werden die vier Kantone Basel-Stadt, Basel-Landschaft, Solothurn und Aargau neu sogenannte ein-

heitliche «Leistungschecks» durchführen:

Die Checks sollen eine unabhängige Standortbestimmung der Schüler(innen)leistungen in den Fächern Deutsch, Mathematik, Fremdsprachen und Naturwissenschaften im 2., 6., 8. und 9. Schuljahr bieten. Für alle teilnehmenden Schüler(innen) eines Schuljahrs gibt es den gleichen Check, der unter denselben Rahmenbedingungen durchgeführt und nach einheitlichen Kriterien extern korrigiert und ausgewertet wird. Dadurch werden die Leistungen unabhängig vom jeweiligen Klassenverband einschätzbar.

Checks und Aufgabensammlung sind Teil eines pädagogischen Konzepts. Die Nutzung ist in ein Qualitätsverfahren eingebunden, welches eine einfache Rückmeldung der Testergebnisse, bedarfsgerechte Weiterbildungen, Handreichungen und Ideensammlung zu Massnahmen umfasst.

Die Auswertung der Prüfungen wird von einem externen Institut wahrgenommen. Es ist somit sicherzustellen, dass die mit diesen Datenbearbeitungen betrauten Personen an datenschutzrechtliche Vorgaben gebunden werden. Die Resultate der Prüfungen, die Vergleiche zwischen Klas-

sen, Schulen und Kantonen werden von diesem Institut an verschiedenste Personen (Lehrkräfte, Schulhausleitungen, Volksschulleitungen usw.) in unterschiedlich aufbereiteter Form übermittelt – auch hier ist sicherzustellen, dass die jeweiligen Empfänger nur jene Daten erhalten, welche sie zu ihrer Aufgabenerfüllung benötigen und dass eine tatsächliche Anonymisierung der Ergebnisse erfolgt. Die vier Kantone sind gemeinsam mit den jeweiligen Datenschutzbeauftragten dabei, Richtlinien auszuarbeiten, um das Risiko von Persönlichkeitsverletzungen zu minimieren.

Canton de Genève

Un projet de loi a été déposé au parlement le 16 octobre 2012¹. Il prévoit deux modifications de la loi actuelle sur l'information du public, l'accès aux données et la protection des données²: d'une part il précise que le secrétariat permanent du préposé cantonal doit être «en principe doté d'au moins un juriste et un collaborateur administratif»³. En cela, le projet de loi est conforme à la position défendue jusque-là par les préposées. D'autre part, il supprime le poste de préposé suppléant pour les raisons suivantes: «Il apparaît notam-



ment que le canton de Genève est le seul canton suisse à prévoir un poste de préposé et un poste de suppléant, alors même que les ressources administratives manquent pour effectuer un travail correct. Cette redondance paraît particulièrement inadaptée en période de restrictions budgétaires et il semble opportun de supprimer le poste de suppléant et de réaffecter les ressources ainsi épargnées à l'engagement d'un/e juriste et d'un/e collaborateur/trice administratif/ve à même d'épauler le suppléant dans ses tâches.» Ce projet de loi sera traité par la commission judiciaire et de police du Grand Conseil. Les préposées demanderont leur audition et défendront que la dotation de quatre postes de travail, pour surveiller notamment l'administration cantonale, les communes, l'aéroport international, l'Université, l'hôpital cantonal, est un minimum absolu pour assurer un travail de qualité.

Kanton Genf

Derzeit wird eine Revision des Genfer «loi sur l'information du public, l'accès aux données et la protection des données»⁴ vom Parlament beraten. Vorgesehen ist zum einen, dass das Sekretariat des bzw. der Datenschutzbeauftragten mit mindestens einem Juristen bzw. einer Juristin sowie einem Verwaltungsassistenten bzw. einer Verwaltungsassistentin ausgestattet sein muss⁵. Diese Änderung steht im Einklang mit der aktuellen Forderung, das Sekretariat bestehen zu lassen.

Hingegen soll die explizite Nennung des Stellvertreters

bzw. der Stellvertreterin des bzw. der Datenschutzbeauftragten gestrichen werden. Dies mit der Begründung, dass der Kanton Genf zum einen als einziger Kanton die Stellvertretung auf gesetzlicher Ebene vorsieht, zum anderen mit dem Argument, dass es angesichts der erforderlichen Budgetkürzungen sinnvoller erscheint, die Stellvertretungsstelle zugunsten eines juristischen Mitarbeiters bzw. einer juristischen Mitarbeiterin und eines Verwaltungsassistenten bzw. einer Verwaltungsassistentin zu streichen und den Stellvertreter bzw. die Stellvertreterin nicht weiter mit diesen Aufgaben zu belasten. Das Gesetzgebungsprojekt wird von der Rechts- und Polizeikommission des Grossen Rates behandelt werden. Die Datenschutzbeauftragten

haben um eine Anhörung gebeten; sie werden sich dafür einsetzen, dass vier Stellen als absolutes Minimum beibehalten werden, um die qualitativ hochwertige Beratung und Kontrolle der kantonalen Verwaltung, der Gemeinden, des internationalen Flughafens, der Universität und des Kantonsspitals sicherzustellen.

Kantone Jura und Neuenburg

Die Parlamente der beiden Kantone haben eine interkantonale Konvention über den Datenschutz und das Öffentlichkeitsprinzip verabschiedet⁶, welche am 1. Januar 2013 in Kraft treten wird. Die Vereinbarung sieht die Einsetzung gemeinsamer Kontrollbehörden im Bereich des Datenschutzes vor (ein[e] Beauftragte[r] sowie eine inter-

Fussnoten

- ¹ <<http://www.ge.ch/grandconseil/data/texte/PL11036.pdf>>.
- ² Loi du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (LIAPD, A 2 08).
- ³ Art. 55, al. 3 LIAPD, nouvelle teneur.
- ⁴ Siehe Fn. 2.
- ⁵ Art. 55 Abs. 3 LIAPD, neue Fassung.
- ⁶ <<http://www.jura.ch/JUST/Commission-cantonale-de-la-protection-des-donnees/Convention-inter-cantonale-JU-NE/Protection-des-donnees-et-transparence-les-cantons-du-Jura-et-de-Neuchatel-renforcent-leur-partenariat.html>>.
- ⁷ LIT, RL 1.6.3.1.
- ⁸ RLIT, RL 1.6.3.1.1.
- ⁹ Regolamento del 5 settembre 2012 sulla gestione dei documenti nell'Amministrazione cantonale, RL 2.5.1.1.6.
- ¹⁰ Legge del 9 marzo 1987 sulla protezione dei dati personali, LPDP, RL 1.6.1.1.
- ¹¹ <http://twitter.com/dsb_zh>.
- ¹² <<http://www.datenschutz.ch>>, Rubrik Veröffentlichungen – Leitfaden und Checklisten.
- ¹³ <<http://www.datenschutz.ch>>, Rubrik Organisation & Technik.
- ¹⁴ <<http://www.datenschutz.ch>>, Rubrik Gemeinden – Informationssicherheit.
- ¹⁵ Datenschutzgesetz vom 14. März 2002, LR 235.1.
- ¹⁶ Strafprozessordnung vom 18. Oktober 1988, LR 312.0.
- ¹⁷ Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABI L 350/2008, S. 60 ff.
- ¹⁸ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABI L 239/2000 S. 1 ff.
- ¹⁹ Bis in die 1990er-Jahre gab es ein öffentliches Verzeichnis aller Autonummern in Liechtenstein.

kantonale Rekurskommission). Zudem sollen einheitliche kommunale Regelungen zum Datenschutz und dem Öffentlichkeitsprinzip geschaffen werden.

Kanton Tessin

Am 1. Januar 2013 werden das neue «Legge del 15 marzo 2011 sull'informazione e sulla trasparenza dello Stato»⁷ und das «Regolamento del 5 settembre 2012 della legge sull'informazione e sulla trasparenza dello Stato»⁸ in Kraft treten. Gleichzeitig wird für die kantonale Verwaltung ein Reglement des Staatsrates⁹ in Kraft gesetzt werden, welches Prinzipien einer korrekten Aktenführung darlegt.

Ebenso wird am 1. Januar 2013 eine Partialrevision des Tessiner Datenschutzgesetzes¹⁰ in Kraft treten. Angepasst werden die Art. 10 und 11 (Bekanntgabe von Personendaten an öffentliche Organe bzw. an Private; mit gleichzeitiger Koordinationsnorm mit dem kantonalen Öffentlichkeitsgesetz), Art. 14 Abs. 3 und 4 (Abrufverfahren) und Art. 25a (Sperrrecht). Mit diesen punktuellen Änderungen wurde eine weitere Harmonisierung mit dem DSG des Bundes angestrebt.

Kanton Zürich

■ Der Datenschutzbeauftragte des Kantons Zürich ist neu mit einem Twitter-Account in den Sozialen Medien präsent¹¹. Über den Twitter-Account soll auf den eigenen Webcontent hingewiesen werden, aber auch auf Inhalte von Experten und/oder Behörden und Institutionen aus der Datenschutz-Community sowie auf relevante Datenschutzzinfos bei Online-Medien. Ein Disclaimer hält die wichtigsten Richtlinien, Hinweise und Vorkehrungen zur sicheren Nutzung von Twitter fest.

■ Der Datenschutzbeauftragte hat einen Leitfaden über den Zugang zu Personendaten Dritter sowie einen Leitfaden zur Sicherheit von Smartphones und Tablets publiziert¹².

■ Des Weiteren stehen überarbeitete Allgemeine Geschäftsbedingungen für die Auslagerung von Informatikleistungen zur Verfügung, welche auch das Cloud Computing berücksichtigen¹³.

■ Für die Gewährleistung der Informationssicherheit bei kleineren Gemeinden und ähnlichen Institutionen stehen neu zahlreiche Vorlagen und Anleitungen zur Verfügung¹⁴. Gleichzeitig werden entsprechende Kurse für diese Zielgruppe angeboten.

Fürstentum Liechtenstein

■ In Liechtenstein sind am 1. Oktober 2012 die Änderungen des DSG¹⁵ und der StPO¹⁶, mit welchen der Rahmenbeschluss¹⁷ zum Datenschutz in der ehemaligen dritten Säule der EU umgesetzt wird, in Kraft getreten: Der Vorbehalt, wonach das DSG in Straf- und Rechtshilfeverfahren nicht anwendbar war, wurde aufgehoben, dafür wurden in der StPO einzelne Datenschutzbestimmungen eingeführt. Der Anwendungsbereich des Datenschutzgesetzes wurde somit wiederholt ausgedehnt. Mit derselben Revision wurden auch Präzisierungen der Umsetzung der EU-Datenschutzrichtlinie¹⁸ vorgenommen. So wurde auch für Unternehmen die allgemeine Pflicht zur Anmeldung von Datensammlungen eingeführt und die Regelung zur vorgängigen Information ausgebaut. Schliesslich gilt fortan, dass das Personal der Datenschutzstelle nicht mehr von der Regierung, sondern durch das Landtagsbüro im Einvernehmen mit dem Datenschutzbeauftragten an-

gestellt wird. Dieser letztere Punkt dient der Stärkung der Unabhängigkeit der Datenschutzstelle von der Regierung.

■ Am 28. Januar 2013 organisiert die Datenschutzstelle zusammen mit dem Institut für Wirtschaftsinformatik der Universität Liechtenstein eine öffentliche Veranstaltung rund um das Thema «der Wert der Privatsphäre». Dabei ist unter anderem geplant, beim Publikum vor Ort eine Umfrage durchzuführen, um den «Puls» zu messen: Was soll privat sein, was nicht? Einträge auf Facebook, die eigene Autonomnummer¹⁹, die Steuererklärung, Gesundheitsangaben usw.? Informationen zur Veranstaltung sind auf der Internetseite der Datenschutzstelle (<<http://www.dss.llv.li>>) verfügbar. ■

Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: zs.verlag@schulthess.com

Homepage: www.schulthess.com

Schulthess 