



## **12. Symposium on Privacy and Security**

Dienstag, 6. November 2007

im Swiss Re Centre for Global Dialogue, Rüslikon/Schweiz

### **Datenschutz und Informationssicherheit in die Prozesse integrieren – Die Herausforderung der Umsetzung**

#### **Summary**

Datenschutz und Informationssicherheit beschäftigen Fachleute, Unternehmen und Verwaltungen seit über zwei Jahrzehnten. Konzepte sind zwar oft vorhanden – aber werden die Ziele von Datenschutz und Informationssicherheit auch tatsächlich und wirksam umgesetzt? Am diesjährigen Symposium on Privacy and Security zogen Experten aus dem In- und Ausland eine gemischte Bilanz: Die Sensibilität für beide Themen ist spürbar gewachsen, die Integration in die Prozesse jedoch ist unterschiedlich weit fortgeschritten. Es bleibt noch viel zu tun.

Eröffnet wurde das Symposium von *Christoph Nabholz* (Head Business Development, Swiss Re Centre for Global Dialogue). Die Grussworte sprach *Regierungsrätin Regine Aeppli* (Vorsteherin der Bildungsdirektion des Kantons Zürich). Selbst im Bildungswesen sei man täglich mit Datenschutzfragen konfrontiert. Sie betonte, dass es auch eine Aufgabe des Bildungssystems sei, Kinder und Jugendliche im Umgang mit neuen Medien und Informationstechnologien in Bezug auf Datenschutz und – persönliche – Informationssicherheit zu beraten und zu unterstützen.

Nach einer kurzen Einleitung ins Thema durch *Beat Rudin* (Stiftung für Datenschutz und Informationssicherheit) eröffnete *Professor Christoph Minnig* (Institut für Personalmanagement und Organisation, Hochschule für Wirtschaft, FH Nordwestschweiz) die Reihe der Referate. Er berichtete über die Schwierigkeit, nicht prioritäre Themen wie Datenschutz und Informationssicherheit «in die Köpfe» der Menschen zu bringen. Die Emotionalität als Bestandteil von Entwicklungsprozessen werde oftmals unterschätzt. Kommunikation – und nicht nur Information – auf allen Ebenen der Führung sei die verbindende Grösse, um Entwicklungen erfolgreich zu gestalten. Nur wer auch die Wirkung von Entwicklungen kenne und nicht nur die Gründe, werde sich ernsthaft damit auseinandersetzen. Das gilt fürs Thema Datenschutz genau so wie für viele andere Projekte.

Die Kommunikation führte auch *Bruno Porro* (Chairman of the Chief Risk Officers Networks, The Geneva Association, und früherer Chief Risk Officer, Swiss Re) als einer der Erfolgsfaktoren für mehr Datenschutz und Datensicherheit an. Damit die Themen nicht nur Floskeln bleiben, brauche es auf Unternehmensebene eine klare Philosophie, die dann auch umgesetzt und angewendet werde. Dass Unterneh-



mensleiter dabei als Vorbilder agieren, sei ebenso eine Voraussetzung wie ein schrittweises Vorgehen bei der Implementierung.

Nach *Oliver Drafi* (Leiter Datenschutz, Allianz Deutschland AG) beruht ein effektives Datenschutz-Management auf drei Erfolgsfaktoren: starke Unterstützung durch die Geschäftsführung, adressatengerechte interne Information und die enge Zusammenarbeit mit anderen Abteilungen wie Recht, IT-Security oder Revision. Die wichtigste Grundvoraussetzung aber seien «privacy-minded people», also für den Datenschutz sensibilisierte Mitarbeitende, die dem Thema auch die notwendige Priorität einräumen.

Syngenta stelle Datenschutz und Informationssicherheit anhand einheitlich strukturierter Prozesse sicher, bei denen die Risikoeinschätzung mit Hilfe von Fragebögen und Checklisten im Zentrum stehe, berichtete *Josef Zehnder* (Leiter Corporate Information Security, Data Protection and Records Retention, Syngenta International AG). Als eine seiner wichtigsten Aufgaben bezeichnete er es, bei den Mitarbeitenden als «Wanderpredigers» unablässig die nötige Aufmerksamkeit für diese Themen einzufordern. Genau so wichtig seien aber auch unangekündigte Kontrollen und das Reporting, wobei die Kontrollen in erster Linie motivierenden und nicht bestrafenden Charakter haben sollen.

Rechtsanwalt *James Thomas Peter* orientierte über die Revision des Datenschutzgesetzes des Bundes, die anfangs 2008 in Kraft treten soll, und über die wesentlichsten Auswirkungen auf die Datenbearbeiter und auf die Informatik. Der Schwerpunkt der Revision liege bei den für Bundesorgane und Private gültigen allgemeinen Grundsätzen. Wichtige Stichworte seien die Erkennbarkeit der Beschaffung von Personendaten und des Zweck ihrer Bearbeitung für die betroffene Person, die Pflicht, betroffene Personen über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren, die präzisere Regelung der grenzüberschreitenden Bekanntgabe von Personendaten und die Möglichkeit der Zertifizierung von Systemen, Verfahren und Organisationen im Datenschutzbereich.

Die Bedeutung solcher Zertifizierungen vertiefte *Bruno Baeriswyl*, dsb zh und Präsident von privatim. Zertifizierungen und Gütesiegel sollen eine Verbesserung des Datenschutzes und mehr Transparenz der Datenbearbeitungen bringen. Sie eigneten sich auch als Ergänzung von bestehenden Zertifizierungen, etwa im Management- und Organisationsbereich. Kritisch äusserte er sich zu den Tatsachen, dass die Zertifizierung nicht durch eine unabhängige Stelle kontrolliert werden solle und dass kein offizielles Qualitätszeichen geschaffen werde, was die tatsächliche Aussagekraft von Gütesiegeln relativieren könne. Zudem vermisste der Referent, dass man sich beim revidierten Datenschutzgesetz des Bundes bezüglich Zertifizierungen und Gütesiegel nicht mehr an internationalen «Best-Practice»-Beispielen orientiert hat.

Die abschliessende Paneldiskussion, an der alle Referenten des Tages teilnahmen, wurde moderiert durch *Marco Marchesi*, CEO ISPN AG, Bassersdorf, Präsident ISSA CH, und *Beat Rudin*. Dabei wurde von verschiedener Seite bemängelt, dass Datenschutz und Informationssicherheit auf Unternehmensebene heute noch allzu oft als



«lästige» Compliance-Aufgabe betrachtet werden. Erst wenn in sensitiven Datenbereichen etwas schief laufe, ändere sich das Verhalten. Daran habe sich auch rund zwei Jahrzehnte nach Beginn der Datenschutzdiskussion kaum etwas geändert. Aus dem Publikum wurde diesen Feststellungen entgegen gehalten, dass bei Unternehmen und in Verwaltungseinheiten durchaus ein Veränderungsprozess stattgefunden habe, zumal die Datenschutzgesetze keine andere Wahl gelassen haben.

Gerade das revidierte Datenschutzgesetz aber wurde mehrfach kritisiert, etwa von *James Thomas Peter*, der das nun angepasste Regelwerk als halbherzige Lösung bezeichnete. Was fehle, sei der nötige Rückhalt aus Wirtschaft, Gesellschaft und Politik, um Datenschutzfragen ernsthaft und umfassend anzupacken.

Als zentralen Erfolgsfaktor für qualitativen Datenschutz und hohe Informationssicherheit hoben die Teilnehmer der Paneldiskussion die Aufgabe hervor, bei den Mitarbeitenden in Unternehmen und Verwaltungen das Bewusstsein und das Verständnis für die Wichtigkeit dieser Themen zu fördern. Dies verlange nach einem anhaltenden Kommunikationsfluss und sei als eine der wichtigsten Führungsaufgaben anzusehen.

Von allen Teilnehmern wurde zudem die Haltung geteilt, dass auch zwei Jahrzehnte nach Beginn der Datenschutzdiskussion in der schweizerischen Öffentlichkeit ein Ende der Vermittlungsarbeit von den Datenverarbeitenden hin zu den von Datenerfassungen betroffenen Personen nicht abzusehen ist. Dabei reichte die Spannweite von resignierender Frage nach dem «Rückwärtsgang» bis zur Überzeugung, dass mit zunehmender Vernetzung und unweigerlich kommenden Schadenfällen eine deutliche Verbesserung der Sensibilisierung einhergehen werde. Begrüsst wurde, dass sich die Diskussion im Laufe der Zeit von einer emotionalen auf eine zunehmend sachliche Ebene verlagert hat – auch wenn die Emotionalität zuweilen immer noch einen hohen Stellenwert einnimmt und die Entwicklungen in Datenschutz und Informationssicherheit davon wohl nie ausgenommen sein werden.

### **Kurz&bündig**

Das SPS 2007 nahm ein «altes» Thema auf: Wie bekommen wir Datenschutz und Informationssicherheit in die Prozesse? Gute Vorsätze und schöne Konzepte garantieren das nicht; es braucht auch weiterhin gewinnende «Wanderprediger». Zertifizierungen können den Prozess unterstützen, wenn sie auf eine Verbesserung zielen und nicht bloss auf die Einhaltung des für alle geltenden Minimalniveaus.