Nummer 12

Tätigkeitsbericht 2006

Datenschutz
mit Qualität

datenschutzbeauftragter
kanton zürich

Nummer 12
Tätigkeitsbericht 2006

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 12 [2006] deckt den Zeitraum vom 1. Januar 2006 bis 31. Dezember 2006 ab.

Der Bericht ist auch auf der Website **www.datenschutz.ch** veröffentlicht.

Zürich, Juni 2007

Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

Inhaltsverzeichnis

IV. SICHERHEIT UND KONTROLLE

V. VERNEHMLASSUNGEN

VI. INFORMATION

VII. ANHANG

Gestärkte Rechte der Bürgerinnen und Bürger

Im vergangenen Jahr konnten die Beratungen über das Informations- und Datenschutzgesetz (IDG) abgeschlossen werden, und am 12. Februar 2007 hat der Kantonsrat das Gesetz in der Schlussabstimmung verabschiedet. Damit wurde die Grundlage für einen zukunftsgerichteten Datenschutz geschaffen.

Das Datenschutzgesetz (DSG) trat 1995 zu einem Zeitpunkt in Kraft, als «Internet» für die meisten noch ein Fremdwort war. Das Ziel des Gesetzes, die Privatsphäre der Bürgerinnen und Bürger vor den zunehmenden Risiken der neuen Technologien für die Persönlichkeitsrechte zu schützen, zeigte sich schon bald als schwierig umzusetzen. Denn die Konzeption des Gesetzes (wie auch der übrigen Datenschutzgesetze in der Schweiz) war den tatsächlichen technologischen Entwicklungen kaum angepasst. Von der Vorstellung der 1960er Jahre geprägt – ein Grosscomputer bearbeitet zentral und kontrolliert die Daten der Bürgerinnen und Bürger – und von den Entwicklungen der 1990er Jahre überrannt – viele dezentrale (Personal) Computer tauschen miteinander schnell und einfach Daten über Netzwerke aus – stellte sich schon bald die Frage, wie das DSG mit Blick auf diese Entwicklungen sinnvoll interpretiert und angewendet werden kann. Gleichzeitig zeichneten sich immer neue Entwicklungen hin zum allgegenwärtigen Computer und zu einer Verselbständigung der Computer ab, an deren Anfang wir heute stehen.

Aber auch auf der gesellschaftlichen Ebene erwies sich das DSG zunehmend als unzureichend. Die Informatisierung der Gesellschaft (und der Verwaltung) brachte eine enorme Zunahme der Datenmengen und des Datenaustausches. Der Bedarf nach Daten wuchs, und der Zugang zu Informationen wurde immer mehr zum strategischen Erfolgsfaktor.

Neuer Ansatz: IDG

In dieser Situation machte der Kanton Zürich einen Schritt nach vorn: Mit dem Informations- und Datenschutzgesetz (IDG) wird einerseits das Datenschutzrecht auf die neuen technologischen Herausforderungen hin angepasst (das DSG wird gleichzeitig ausser Kraft treten), und andererseits wird der Umgang mit Informationen umfassend geregelt.

Auf der einen Seite sind die Rahmenbedingungen, wie sie im neuen Gesetz für die Technologie geschaffen wurden, risikoorientiert und auf Schutzziele ausgerichtet: Der Einsatz neuer Technologien hat diese Schutzziele und damit einen korrekten Umgang mit den Daten der Bürgerinnen und Bürger zu gewährleisten. Je höher das Risiko für die Persönlichkeitsrechte ist, desto höhere Anforderungen sind an die organisatorischen und technischen Massnahmen zur Verringerung der Risikosituation zu stellen. Im Vordergrund steht dabei der Einsatz von

datenschutzfreundlichen Technologien und Verfahren. Gleichzeitig wird den datenbearbeitenden Stellen die Möglichkeit eröffnet, ihre Verfahren und technischen Einrichtungen zertifizieren zu lassen, um so gegen aussen belegen zu können, dass die geeigneten Massnahmen zum Schutz der Privatheit der Bürgerinnen und Bürger getroffen wurden. Insbesondere beim elektronischen Datenaustausch im Rahmen des E-Government kann dadurch vermehrt Vertrauen geschaffen werden.

Auf der anderen Seite werden Informationen und Daten in ihrem Kontext betrachtet – von der Entstehung bis zur Archivierung –, und auch hier konnten klare Rahmenbedingungen geschaffen werden. Der Umgang mit Informationen ist die Basis, auf der die spezifischen Bestimmungen für das Bearbeiten von Personendaten und besonderen Personendaten wie Daten aus dem Gesundheitswesen aufbauen. Wiederum steht die risikobezogene Betrachtung im Vordergrund, indem die Voraussetzungen für das Bearbeiten von Personendaten und besonderen Personendaten im Gesetz klar festgelegt sind.

Erhöhte Transparenz

Das Bearbeiten von Personendaten ist grundsätzlich erlaubt, wenn die Daten im Rahmen der gesetzlich umschriebenen Aufgabenerfüllung geeignet und erforderlich sind. Hingegen sind besondere Personendaten einer erhöhten Transparenz unterworfen. Da bei diesen Daten ein grösseres Risiko für die Persönlichkeitsrechte der betroffenen Personen besteht, ist deren Bearbeitung an das Vorliegen eines formellen Gesetzes gebunden. Des Weiteren ist bei der Beschaffung von besonderen Personendaten die datenbearbeitende Stelle verpflichtet, die betroffenen Personen über den Zweck der Datenbearbeitung zu informieren. Damit wird bei diesen Daten einerseits die Legitimation des Eingriffs in die Privatheit einer stärkeren demokratischen Kontrolle unterworfen und andererseits – wie erwähnt – die Transparenz der Datenbearbeitungen erhöht.

Auch im Rahmen der Bekanntgabe von Informationen nach dem Öffentlichkeitsprinzip sind die Rechte auf Privatheit der betroffenen Personen gewährleistet. Soll auf dieser Grundlage Zugang zu Personendaten eröffnet werden, ist die betroffene Person anzuhören. Besondere Personendaten dürfen dabei nur mit einer Einwilligung bekannt gegeben werden. Mit diesen Bestimmungen wird auch hier konsequent eine risikobezogene Interessenabwägung vorgenommen.

Individuelle Rechte

Nach wie vor im Mittelpunkt der individuellen Rechte steht das jeder Person zustehende Auskunftsrecht. Damit wird ihr jederzeit ermöglicht, sich ein Bild darüber machen zu können, welche Daten über sie von einer bestimmten Verwaltungsstelle bearbeitet werden. Stellen sich diese Daten als falsch heraus oder besteht keine Grundlage für deren Bearbeitung, ist es möglich, eine Berichtigung oder Löschung der Daten zu verlangen. Ausdrücklich wird im IDG nun auch statuiert, dass dieses Auskunftsrecht kostenlos gewährt werden muss.

Neben dem Recht auf Auskunft über die eigenen Daten steht den Bürgerinnen und Bürgern als Kern des Öffentlichkeitsprinzips auch ein individuelles Recht auf Zugang zu Informationen der Verwaltung zu. Dieses Recht ist nicht Teil der datenschutzrechtlichen Ansprüche, sondern ist als Konsequenz der demokratischen Mitwirkungs- und Kontrollrechte der Bürgerinnen und Bürger zu verstehen.

Aufsichtsorgan mit neuen Kompetenzen

Weil die Datenbearbeitungen immer komplexer werden und damit auch immer mehr Risiken für die Privatheit der Bürgerinnen und Bürger umfassen, weist das IDG auch neue Kompetenzen für den Datenschutzbeauftragten auf. Einerseits ist der Kanton Zürich aufgrund der Abkommen von Schengen und Dublin sowie der Ratifizierung eines Zusatzprotokolls zur Konvention des Europarates über den Schutz der Menschen bei der automatisierten Bearbeitung von Personendaten verpflichtet, die Gesetzgebung anzupassen. Andererseits sind die einzelnen Bürgerinnen und Bürger mit der Kontrolle der Datenbearbeitungen auf der generellen Ebene überfordert. Deshalb wurde insbesondere der Bereich der Kontrolltätigkeit verstärkt. Im Rahmen so genannter Vorabkontrollen sind dem Datenschutzbeauftragten alle Vorhaben zur Prüfung zu unterbreiten, die ein besonderes Risiko für die betroffenen Personen beinhalten. Damit soll von Anfang an gewährleistet werden, dass die Anliegen des Datenschutzes angemessen in diese gesetzgeberischen und anderen Projekte einfliessen. Nicht zuletzt ist dies auch verwaltungsökonomisch sinnvoll, ist es doch immer aufwändiger und teurer, ein Projekt nachträglich an die Erfordernisse des Datenschutzes anpassen zu müssen.

Des Weiteren kann der Datenschutzbeauftragte aufgrund des IDG Empfehlungen, die von einer Verwaltungsstelle abgelehnt oder nicht umgesetzt werden, einer gerichtlichen Instanz zum Entscheid vorlegen. Damit kann gewährleistet werden, dass die datenschutzrechtlichen Vorgaben auch tatsächlich eingehalten werden und sich eine Verwaltungsstelle auch an den übergeordneten Interessen – dem Schutz der Privatheit der Bürgerinnen und Bürger – mit der gleichen Konsequenz zu orientieren hat wie an ihren eigenen Interessen. Dass diese eigentlich deckungsgleich sein sollten und deshalb diesbezüglich keine Probleme auftreten sollten, war in der Vergangenheit nicht immer selbstverständlich. Es ist deshalb zu begrüssen, dass nun in Abwägung der Interessen der Bürgerinnen und Bürger verbindliche Anordnungen getroffen werden können.

Zunehmende Herausforderungen

Wie auch der vorliegende Tätigkeitsbericht zeigt, sind die Herausforderungen für den Schutz der Privatheit der Bürgerinnen und Bürger nach wie vor vielfältig. Nicht nur die technische Entwicklung, sondern auch immer grössere und umfassendere Datenbearbeitungen verlangen eine konsequente Umsetzung der datenschutzrechtlichen Rahmenbedingungen.

Mit dem Anschluss an das Schengener Informationssystem wird im polizeilichen Bereich ein Fahndungssystem von bisher unbekanntem Ausmass für die Schweiz geschaffen. Die Europäische Union (EU) als verantwortliche Stelle für dieses Fahndungssystem hat zahlreiche Massnahmen getroffen, um die Privatheit der Bürgerinnen und Bürger zu schützen. Auch in der Schweiz und im Kanton Zürich sind diese Massnahmen konsequent umzusetzen, damit der gleiche Schutz wie für die EU-Bürger auch für die Schweizer Bürgerinnen und Bürger gewährleistet werden kann. Dies erfordert insbesondere den Ausbau der Kontrollen durch den Datenschutzbeauftragten, was neben den erfolgten gesetzlichen Anpassungen aber mittelfristig auch vermehrter Ressourcen bedarf.

Ebenso zeigt sich, dass die Sensibilität der Datenbearbeitungen im Gesundheitswesen mit den technologischen Entwicklungen und mit der Zunahme des Datenaustausches weiter wächst. Hier gilt es vor allem durch Beratungen bei der

Gesetzgebung oder in einzelnen Projekten rechtzeitig die notwendigen Vorkehrungen für den Schutz des Patientengeheimnisses treffen zu können.

Im Übrigen treten in allen Bereichen zunehmend komplexere Fragestellungen auf, und auch hier besteht ein grosser Bedarf an Beratung. Insbesondere Gemeinden und kleinere Amtsstellen, die nicht über ausgebaute Rechtsstäbe verfügen, nehmen in diesem Bereich die Dienstleistungen des Datenschutzbeauftragten in Anspruch. Immer mehr wenden sich aber auch Bürgerinnen und Bürger direkt an den Datenschutzbeauftragten. Neben der Beratung dieser Personen sind vielfach auch Vermittlungen gefragt, um einen Ausgleich der Interessen der Bürgerinnen und Bürger am Schutz ihrer Privatheit mit den Absichten der Verwaltungsstellen zu finden. Nicht immer ist ersichtlich, warum eine Verwaltungsstelle bestimmte Daten benötigt, und oft ergibt eine nähere Betrachtung, dass gewisse Daten gar nicht notwendig sind. Dabei kann es sich auch um für die betroffene Person höchst sensible Daten handeln, weshalb der Verzicht auf deren Bearbeitung meistens zu einer erfolgreichen Vermittlung durch den Datenschutzbeauftragten in diesen Fällen führt. Vielfach werden in Formularen zur Abklärung von Eignungen von Personen zu bestimmten Tätigkeiten, beispielsweise im Schulbereich, auch Daten erfragt, die gar nicht notwendig sind.

Auch die regelmässig durchgeführten Datenschutzreviews im technischen Bereich zeigen, dass hier nach wie vor ein grosser Handlungsbedarf besteht. Der Datenschutzbeauftragte ist bemüht, mit seinen Beratungen und Kontrollen zu einem angemessenen Sicherheitsniveau in der gesamten Verwaltung beizutragen. Dies ist nicht nur im Interesse der betroffenen Personen, sondern auch im Interesse der Verwaltung.

«Hautnahe» Technologien

Mit dem Einsatz von Pervasive Computing und der Verwendung von Hirnbildern (Neuroimaging) werden die Datenbearbeitungen im Gesundheitswesen immer sensitiver. Diese «hautnahen» Technologien brauchen deshalb eine enge datenschutzrechtliche Begleitung.

Mit Pervasive Computing wird ein Technologietrend umschrieben, wonach immer kleinere und unauffälligere Chips und Computer immer mehr Daten und Informationen austauschen und auch Handlungen auslösen können. Solche Chips können sich beispielsweise in Gegenständen oder unter der Haut des Menschen befinden. Technologische Entwicklungen, die eine weitergehende Miniaturisierung sowie eine neue Kommunikations- und Sensortechnologie beinhalten, sollen dies ermöglichen. Diese Allgegenwärtigkeit des Computers (Ubiquitous Computing) ist in einer ersten Stufe bereits marktfähig geworden mit der so genannten «Radio Frequency Identification» (RFID): Kleine, unsichtbare Chips, welche heute vorwiegend in Gegenständen untergebracht sind, enthalten Informationen, die sie beim Passieren eines Lesegerätes weitergeben. So können bereits heute Ausweispapiere wie Pässe mit solchen Chips ausgerüstet werden.

Der Einsatz von Pervasive Computing im Gesundheitswesen gilt als besonders zukunftsträchtig. So wird der permanente Informationsaustausch im Rahmen von E-Health-Anwendungen als Chance für die Verbesserung der Behandlungsqualität gesehen: Ein konstantes Monitoring von Patienten, das Lebensgewohnheiten und weitere Einflüsse umfasst, ermöglicht eine zielgerichtete Behandlung. Mit einer laufenden Diagnostik am Körper der Patientin und einem System von ständigen Feedbacks aufgrund von automatisierten oder menschlichen Eingriffen auf die Systeme entsteht eine umfassende Bearbeitung sensitiver Gesundheitsdaten.

Mitbestimmung der Patienten

Im Rahmen einer von der Stiftung Risiko-Dialog, der Stiftung für Datenschutz und Informationssicherheit und von ICT Switzerland initiierten und breit unterstützten Diskussion über die Chancen und Risiken von Pervasive Computing sind drei Teilbereiche diskutiert worden: Detailhandel, öffentlicher Verkehr und Gesundheitswesen. Der Datenschutzbeauftragte hat im Teilbereich Gesundheitswesen mitgewirkt.

Die Gewährleistung der informationellen Selbstbestimmung ist im Gesundheitsbereich eine besondere Herausforderung. Bevor Pervasive Computing eingesetzt wird, ist eine umfassende Aufklärung des Patienten unabdingbar: Er soll darüber informiert werden, welche Daten erhoben werden, wie diese verarbeitet und ob diese allenfalls an Dritte weitergegeben werden. Der Patient hat dabei explizit einzuwilligen, wobei diese Einwilligung generell oder im Einzelfall erfolgen soll. Je nach Konstellation sind Wahlmöglichkeiten («Opt-in» oder «Opt-out») zu gewährleisten. Da sich im Rahmen von Pervasive Computing auch Persönlichkeitsprofile bilden, sollen die Patienten regelmässig über die Daten aufgeklärt werden, die über sie gespeichert werden.

Ein weiterer entscheidender Punkt beim Pervasive Computing im Gesundheitsbereich ist die Möglichkeit für die Patientinnen, jederzeit über die Anwendungen selbständig entscheiden zu können: Es soll in der Autonomie der Patienten liegen, die Systeme ganz oder teilweise zu steuern und so die Entscheidungsgewalt über ihre «automatisierte» Behandlung zu behalten.

Dieser Risikodialog gab viele Anregungen für die datenschutzrechtlichen Herausforderungen, die weit über den Gesundheitsbereich hinausgehen. Es wird nun darum gehen, Lösungen zu finden, wie die Risiken für die Privatheit der betroffenen Personen zu minimieren sind.

Hochsensibles Neuroimaging …

Mit Hightech-Geräten lassen sich aufgrund komplexer Berechnungen farbige Bilder des Gehirns erzeugen. Diese ermöglichen neue Erkenntnisse über das Gehirn und seine Funktionsweise. TA-Swiss, das Zentrum für Technologiefolgen-Abschätzung, hat erstmals eine umfassende Studie über die Chancen und Risiken dieser Technologie publiziert.

Welche Erkenntnisse Neuroimaging in Zukunft noch bringen kann, ist offen. Doch bereits heute zeigt sich, dass die Informationen sehr sensibel sein können. Denn Neuroimaging generiert Daten, die eventuell Rückschlüsse auf Hirnkrankheiten, Funktionsstörungen, Persönlichkeitsmerkmale oder auf normabweichendes Verhalten ermöglichen können. Datenschutzrechtlich ist deshalb entscheidend, zu welchem Zweck, durch wen und unter welchen Bedingungen solche Daten erhoben, ausgewertet und genutzt werden dürfen. Weil Diskriminierungen aufgrund solcher Erkenntnisse oder Datenmissbrauch nicht auszuschliessen sind, braucht es klare Leitplanken für die Verwendung von Neuroimaging.

… auf Forschung und Medizin beschränken

An einer Tagung von TA-Swiss über die Konsequenzen von Hirnbildern für Strafrecht und Datenschutz beschäftigte sich der Datenschutzbeauftragte eingehend mit den datenschutzrechtlichen Fragestellungen. Aus seiner Sicht sind bei der Schaffung von Leitplanken für den Einsatz von Neuroimaging folgende Überlegungen zu beachten:

Die «Bilder», welche durch Neuroimaging erzeugt werden, weisen für die betroffenen Personen eine hohe Sensibilität auf. Die Messwerte, die zu Hirnbildern zusammengefügt werden, zeichnen primär Hirnaktivitäten auf. Der Nutzen dieser Informationen im medizinischen Umfeld ist unbestritten. Die Interpretation dieser Daten über dieses Gebiet hinaus zur Feststellung von Hirnaktivitäten und Persönlichkeitsmerkmalen ist indessen äusserst spekulativ. Und für die betroffenen Personen ist sie mit hohen Risiken für ihre Persönlichkeitsrechte verbunden.

Die technologischen und gesellschaftlichen Trends zeigen, dass das Risikopotenzial enorm ist. Die Technologie ermöglicht die zunehmende Vernetzung von allem mit allem (Ubiquitous Computing) sowie die Aufzeichnung und Aufbewahrung aller Daten und deren unbeschränkte Auswertung. Gesellschaftliche Entwicklungen zeigen, dass schon heute Daten aus allen verfügbaren Quellen zu riesigen Datenbanken akkumuliert werden (Data Warehousing), um sie dann, aus dem Zusammenhang genommen, neu zu kombinieren und damit Personen zu bewerten und zu kategorisieren (Data Mining). Gerade in Bereichen wie Marketing oder Pädagogik, die nach zusätzlichen Quellen für die Kategorisierung von Personen suchen, sind Hirnbilder eine gefährliche Munition.

Aus Sicht der menschlichen Würde und der persönlichen Freiheit ist die Anwendung des Neuroimaging auf die Bereiche Medizin und Forschung zu beschränken. Da darüber hinaus keine verlässlichen Aussagen möglich sind, erscheinen Hirnbilder in anderen Bereichen heute als ungeeignet und nicht erforderlich. Personen, die in die Erstellung von Hirnbildern einwilligen, sind vorher über die möglichen Aussagen aufzuklären. Die Datenschutzgesetzgebung ist bereichsspezifisch zu konkretisieren.

Die im Text erwähnten Studien sind abrufbar unter:

- http://www.risiko-dialog.ch/Publikationen/Kompass.pdf
- http://www.ta-swiss.ch/a/biot_hirn/2006_50A_KF_neuroimaging_d.pdf

Einsatz personaldiagnostischer Instrumente

Mit personaldiagnostischen Instrumenten bei Rekrutierungsverfahren oder in der Personalentwicklung werden Persönlichkeitsprofile erstellt. Für deren Bearbeitung müssen Richtlinien sowie Zugriffskonzepte ausgearbeitet werden, und das Testverfahren muss für die Kandidaten transparent sein.

Ob per Fragebogen oder Assessment Center: Personaldiagnostische Instrumente dienen zur Einschätzung von Personen. Sie können im Rahmen eines Rekrutierungsverfahrens oder in der Personalentwicklung eingesetzt werden. Im Amt für Justizvollzug wurde in einem Pilotprojekt während eines Jahres das personaldiagnostische Instrument «Master Person Analysis» (MPA) eingesetzt. Das MPA besteht aus einem Fragebogen mit rund 40 Fragen. Damit werden die Verhaltensneigungen einer Person, die für die berufliche Tätigkeit relevant sind, erfasst. Zusammen mit einem Anforderungsprofil wird damit ein Bild der Persönlichkeit hinsichtlich einer spezifischen Stelle oder Aufgabe erstellt. Das personaldiagnostische Instrument basiert auf einer strukturierten Selbsteinschätzung der Testperson und wird nach der Auswertung durch einen geschulten und zertifizierten Anwender als Basis für ein Bewerbungsgespräch oder eine Standortbestimmung verwendet. Die Testberichte finden keinen Eingang in die Personalakten.

Mit Blick auf die Einführung solcher personaldiagnostischer Testverfahren im Amt für Justizvollzug und allenfalls in weiteren Amtsstellen hat der Datenschutzbeauftragte folgende Grundsätze festgehalten:

Gesetzliche Grundlage

Mit personaldiagnostischen Testverfahren werden Persönlichkeitsprofile erstellt. Dabei handelt es sich um besonders schützenswerte Personendaten (§ 2 lit. d DSG), deren Bearbeitung erhöhten Anforderungen untersteht. Im Rahmen der Neubesetzung einer Stelle bildet das Personalgesetz (§§ 10 und 34) die gesetzliche Grundlage für solche Eignungstests. Für jeden anderen Einsatz, wie zur Standortbestimmung oder zur Laufbahnberatung, fehlen entsprechende gesetzliche Bestimmungen. Ein solcher Einsatz ist daher nur im Einzelfall mit Zustimmung der Testperson erlaubt. Weigert sich eine Person, einen Persönlichkeitstest für eine Standortbestimmung oder eine Laufbahnberatung zu absolvieren, dürfen ihr daraus keine Nachteile entstehen.

Erhebung und Auswertung

Werden im Rahmen der Rekrutierung Persönlichkeitsprofile mit personaldiagnostischen Instrumenten erhoben, ist gestützt auf den Grundsatz der Verhältnismässigkeit der Test nur bei den Bewerbern durchzuführen, die in die engere Auswahl für eine Anstellung kommen. Der Grundsatz der Verhältnismässigkeit verlangt, dass nur geeignete und erforderliche Daten erhoben werden (§ 4 Abs. 3 DSG). Die Datenerhebung sollte wenn möglich pseudonymisiert erfolgen – beispielsweise durch Vergabe einer Nummer. Die Pseudonymisierung ist besonders dann sicherzustellen, wenn die Auswertung des Tests durch beauftragte Dritte erfolgt oder andere Amtsstellen auf die Daten zugreifen können.

Aufbewahrungsdauer und -ort

Bei Nichteinstellung sind die erhobenen Daten den betroffenen Personen auszuhändigen oder zu vernichten, wenn sie der weiteren Aufbewahrung nicht zustimmen (§ 34 Personalgesetz). Bei Anstellung der Person erscheint eine Aufbewahrungsdauer von zwölf Monaten als angemessen. Wegen ihrer Sensitivität sind die Testergebnisse in einem verschlossenen Couvert (Nebendossier) abzulegen.

Werden die Tests nicht im Zusammenhang mit einer Rekrutierung durchgeführt, hängt die Aufbewahrung von der Zustimmung der Testperson ab. Stimmt sie der Aufbewahrung nicht zu, sind ihr sämtliche Testergebnisse auszuhändigen oder sie müssen vernichtet werden.

Richtlinien und Zugriffskonzept

Eignungstests lassen Raum für Interpretationen. Für Testanwender und Linienvorgesetzte sind deshalb detaillierte Richtlinien auszuarbeiten, wie die Auswertung zu beurteilen ist. In den Richtlinien sollte das personaldiagnostische

Instrument beschrieben und die Verfahren sollten während der Testphase und nach Abschluss der Auswertung festgehalten werden. Festzuhalten ist zudem:

- Das Einsatzgebiet des Tests sowie allfällige Konsequenzen bei Nichtteilnahme im Rahmen von Rekrutierungsverfahren: Verweigert eine Mitarbeiterin im Zusammenhang mit ihrer Laufbahnplanung, Mitarbeiterbeurteilung etc. die Teilnahme an einem solchen Test, dürfen ihr daraus keine Nachteile entstehen.
- Zweckbindung: Die Testresultate dürfen nur als Diskussionsgrundlage für ein vertieftes Gespräch im Rahmen des Testzwecks dienen. Ohne Einwilligung der Testperson dürfen die Daten nicht für andere Zwecke verwendet werden.
- Organisation und Verantwortlichkeiten bei der Testdurchführung: Es ist festzuhalten, wer ermächtigt ist, den Test durchzuführen, ihn auszuwerten und das Feedbackgespräch zu führen.

Zusätzlich zu den Richtlinien ist ein Zugriffskonzept zu erstellen, das festlegt, wer auf welche Daten zugreifen kann und welche Rechte (Lese-, Schreib-, Änderungsrechte etc.) er dabei hat.

Transparenz gegenüber der Testperson

Werden personaldiagnostische Instrumente eingesetzt, müssen die Testpersonen vorgängig umfassend und transparent über die Datenerhebung und Datennutzung informiert werden. Folgende Punkte müssen transparent sein:

- Ziel und Zweck des Einsatzes eines personaldiagnostischen Instruments im konkreten Fall
- Bei Rekrutierung: Hinweis auf gesetzliche Grundlagen im Personalgesetz
- Bei Standortbestimmung und Laufbahnberatung: Hinweis auf Freiwilligkeit und Verweigerungsmöglichkeit ohne Nachteile
- Informationen über Zugriffsrechte und Datenempfänger
- Aufklärung über Auskunftsrechte (inkl. Herausgabe von Kopien) und Berichtigungsrechte
- Aufbewahrungsdauer der Unterlagen

Datensicherheit und Outsourcing

Die Bearbeitung von Persönlichkeitsprofilen stellt erhöhte Anforderungen an die Datensicherheit. Die Daten müssen mit entsprechenden Sicherheitsmassnahmen vor unbefugtem Zugriff geschützt werden, unabhängig davon, ob der Test in Papierversion oder über Internet durchgeführt wird. Die Daten dürfen zudem nur über eine sichere und verschlüsselte Verbindung elektronisch übermittelt werden.

Falls andere Amtsstellen oder IT-Dienstleister für Wartungsarbeiten oder Auswertungen auf Personendaten zugreifen können, sind gemäss § 13 DSG die entsprechenden organisatorischen und technischen Massnahmen (http://www.datenschutz.ch/themen/1161.php) zu ergreifen. Allenfalls sind die AGB Sicherheit des Kantons Zürich (http://www.datenschutz.ch/themen/2001_agb_sicherheit.pdf) in die Verträge mit den amtsexternen Dienstleistern zu integrieren.

Schulung

Werden personaldiagnostische Instrumente eingesetzt, müssen sämtliche Personen, die mit der Auswertung befasst sind, für die richtige Handhabung und Interpretation der Tests geschult werden. Auch Linienvorgesetzte, welche die Testergebnisse ebenfalls zur Kenntnis nehmen, müssen die Auswertungen richtig interpretieren und anwenden können.

Forschung mit Personendaten

Die staatlichen Behörden verfügen über Datenbestände, die wertvolle Informationen für die Forschung liefern können. Das Datenschutzgesetz sieht gewisse Erleichterungen für die Datennutzung zu Forschungszwecken vor. Im Bereich der medizinischen Forschung gelten zusätzlich Bestimmungen des Strafgesetzbuches.

Bei der Erhebung von Personendaten zu Forschungszwecken stellen sich immer wieder datenschutzrechtliche Fragen bezüglich der Datenweitergabe durch öffentliche Organe und der Einwilligung der betroffenen Personen. In diesem Zusammenhang wurde der Datenschutzbeauftragte in mehreren Fällen sowohl von den angefragten Behörden als auch von Personen, die in ein Forschungsprojekt involviert waren, kontaktiert. Fragen zur Rechtmässigkeit der Datenerhebung und Einwilligung standen jeweils im Zentrum.

Die wissenschaftliche Forschung, beispielsweise an Universitäten und Fachhochschulen, liegt im Interesse der Allgemeinheit. Entsprechend ist in Art. 20 Bundesverfassung die Wissenschaftsfreiheit verankert. Diese gilt jedoch nicht uneingeschränkt. Denn bei der Forschung mit Personendaten kollidieren die Interessen der Forschung am uneingeschränkten Zugang zu Informationen mit den Interessen der betroffenen Personen punkto Persönlichkeitsschutz. Eine Interessenabwägung der angestrebten Forschungsziele mit dem Eingriff in die Persönlichkeitsrechte der Betroffenen ist deshalb unabdingbar. Sowohl die Datenschutzgesetzgebung als auch das Strafgesetzbuch enthalten Bestimmungen, in denen diese Interessenabwägung zum Teil schon vorgenommen wurde.

Erleichterte Datenbearbeitung für Forschung

Staatliche Organe wie Spitäler oder Schulbehörden verfügen über eine Vielzahl von Personendaten, die wertvolle Erkenntnisse für die Forschung, Planung oder Statistik liefern können. Da in diesen Bereichen nicht die Angaben über eine konkrete Einzelperson von Interesse sind, erlaubt die Datenschutzgesetzgebung den staatlichen Organen die so genannte «nicht personenbezogene Datenbearbeitung» unter erleichterten Bedingungen (vgl. § 12 DSG). Folgende Bestimmungen werden dabei aufgehoben: das Zweckbindungsgebot (§ 4 Abs. 4 DSG), das Erfordernis der formell-gesetzlichen Grundlage für die Bearbeitung besonders schützenswerter Personendaten (§ 5 DSG) und die gesetzliche Grundlage für die Bekanntgabe von Personendaten (§ 8 Abs. 2 DSG).

Personendaten dürfen gemäss § 12 DSG für nicht personenbezogene Zwecke, insbesondere in der Forschung, Planung und Statistik, unter folgenden Bedingungen bearbeitet werden: Die Daten müssen anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, und die Ergebnisse müssen so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind (Abs. 1). Die erleichterten Bedingungen gelten, wenn das verantwortliche öffentliche Organ selbst «eigene» Bestände von Personendaten zu nicht personenbezogenen Zwecken bearbeitet. Der Persönlichkeitsschutz wird hier durch das Erfordernis der frühestmöglichen Anonymisierung und der Veröffentlichung ohne Personenbezug gewährleistet.

Ebenfalls erleichterten Bedingungen untersteht die Bekanntgabe von Personendaten an Dritte. Öffentliche Organe wie Universitätskliniken oder Schulbehörden dürfen Personendaten zu nicht personenbezogenen Zwecken Dritten, wie Forschenden oder Doktorierenden, bekannt geben, wenn keine Geheimhaltungspflicht (vgl. «Sonderfall bei Forschung mit medizinischen Daten») oder andere Bestimmung dies ausschliesst und Rückschlüsse auf die betroffenen Personen möglichst erschwert sind (Abs. 2).

Da in diesem Fall Daten an Dritte gelangen und das Organ, das die Daten herausgibt, weiterhin für die Einhaltung des Datenschutzes verantwortlich ist, ist die angefragte Behörde gut beraten, zusätzliche Bedingungen zu beachten: Forschungsgesuche Dritter sollten schriftlich an die Behörden gestellt werden. Die angefragte Behörde darf die Bewilligung nur mit klaren Rahmenbedingungen, die den Datenschutz gewährleisten, erteilen. Heikel ist zudem, wenn ein staatliches Organ Adressdaten, beispielsweise von Personen, die sich in psychiatrischer Be-

handlung befinden oder die strafrechtlich verfolgt wurden, an Forschungsstellen oder Doktorierende herausgibt, die dann selber diese Personen anfragen, ob sie an einem Forschungsprojekt teilnehmen möchten. Sollen betroffene Personen aktiv in die Forschungsarbeit einbezogen werden, sollte insbesondere bei der Erhebung besonders schützenswerter Personendaten die erste Kontaktaufnahme über das Organ erfolgen, das über die Datenbestände verfügt und für die Gewährleistung der rechtmässigen Bearbeitung der Personendaten verantwortlich ist. Bei Forschungsprojekten, bei denen Jugendliche oder Minderjährige einbezogen werden, muss je nach Forschungsinhalt zusätzlich die Einwilligung der Eltern eingeholt werden.

Sonderfall bei Forschung mit medizinischen Daten

Auch für die medizinische Forschung gelten die Erleichterungen zur Datenbearbeitung oder -bekanntgabe gemäss § 12 DSG. Soll Dritten im Rahmen eines Forschungsprojektes aber Einsicht in medizinische Patientendossiers gewährt oder sollen medizinische Daten bekannt gegeben werden, ist – sofern keine Einwilligung der betroffenen Personen vorliegt – ein besonderes Verfahren einzuhalten, wenn sich die Daten im Besitz eines Arztes oder einer anderen an das Berufsgeheimnis gebundenen Person befinden: In diesem Fall muss bei der Sachverständigenkommission zur Aufhebung des Berufsgeheimnisses (Art. 321bis StGB) ein Gesuch um Aufhebung des Berufsgeheimnisses eingereicht werden. Die Sonderbewilligung wird erteilt, wenn die Forschung nicht mit anonymisierten Daten erfolgen kann, die Einwilligung der betroffenen Personen nicht mehr oder nur mit unverhältnismässig hohem Aufwand eingeholt werden kann und die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen. Vorausgesetzt ist zudem, dass die betroffene Person zu einem früheren Zeitpunkt die Verwendung ihrer Daten zu Forschungszwecken nicht ausdrücklich untersagt hat.

Die Sachverständigenkommission verbindet die Bewilligung zur Sicherstellung des Persönlichkeitsschutzes der Betroffenen mit datenschutzrechtlichen Auflagen, beispielsweise zur Datensicherheit. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte überprüft, ob die Auflagen der Sachverständigenkommission eingehalten werden. Für die Datenbekanntgabe und die Einhaltung der Bestimmungen des § 12 DSG ist der Datenschutzbeauftragte des Kantons Zürich zuständig.

Kein Problem bei anonymisierten Daten

Sind Personendaten vor Beginn des Forschungsvorhabens bereits rechtskonform anonymisiert, kommen die vorliegenden Bestimmungen des DSG und StGB nicht mehr zum Tragen. Denn reine Sachdaten oder Sachinformationen fallen nicht in den Anwendungsbereich des DSG. Sind die Forschungsdaten hingegen pseudonymisiert, kommen die Bestimmungen des DSG zur Anwendung, da – zumindest indirekt – nach wie vor Rückschlüsse auf die betroffenen Personen möglich sind.

Videoüberwachung im öffentlichen Verkehr

Nach Pilotversuchen durch den Zürcher Verkehrsverbund (ZVV) sind Videoüberwachungsmassnahmen mit der neuen Verordnung per 1. Januar 2007 definitiv eingeführt worden: tagsüber und im Nachtnetz punktuell auf bestimmten Linien und bei bestimmten Haltestellen.

Wegen der zunehmenden Bedeutung des Themas Sicherheit im öffentlichen Personenverkehr in den letzten Jahren beauftragte der Kantonsrat mit Beschluss der Strategie 2005 bis 2008 den ZVV, wirksame Massnahmen in den Bereichen Sicherheit, Sauberkeit und Vandalismus zu ergreifen. Das erarbeitete Massnahmenpaket sah auch Pilotversuche für eine Videoüberwachung vor. Der Datenschutzbeauftragte war in die Erarbeitung der Richtlinien vom 15. Dezember 2003 involviert. Ebenso verfasste er eine Stellungnahme zum Entwurf der Verordnung über die Videoüberwachung im öffentlichen Verkehr. Die Verordnung berücksichtigt die datenschutzrechtlichen Vorgaben weitgehend.

Die Verordnung richtet sich an die Verkehrsunternehmen, die im Auftrag des ZVV das Netz des öffentlichen Personenverkehrs betreiben und für die Umsetzung der Sicherheitsziele verantwortlich sind. Der ZVV erteilt ihnen auf deren Gesuch hin eine Bewilligung, welche die Rahmenbedingungen für den Betrieb der Videoüberwachung festlegt. Um Transparenz zu schaffen und die präventive Wirkung zu verstärken, sind die Verkehrsunternehmen verpflichtet, die Fahrzeuge und Haltestellen mit Videoüberwachung zu kennzeichnen und eine Kontaktstelle für Anfragen bekannt zu geben.

Nicht anwendbar ist die Verordnung auf die Schweizerischen Bundesbahnen (SBB), die den grössten Teil des Zürcher S-Bahn-Systems betreiben. Sie unterstehen einer ähnlichen Verordnung des Bundes.

Klare Zweckbindung

Die Videoüberwachung erfasst Bilder von Personen und registriert deren Verhalten. Dadurch können Personendaten und sogar Persönlichkeitsprofile erhoben werden (§ 2 der Verordnung und § 2 lit. e und f DSG). Die Videoüberwachung beeinträchtigt somit die Grundrechte von Bürgerinnen und Bürgern. Betroffen sind neben Reisenden auch Besucherinnen und Besucher von Anlagen sowie Fahr- und Betriebspersonal der Verkehrsunternehmen. Datenbearbeitungen, die in die Persönlichkeitsrechte eingreifen, unterliegen einer klaren Zweckbindung: Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird (§ 4 Abs. 4 DSG). Die Verordnung hält fest, dass die Videoüberwachung nur zum Schutz der Reisenden sowie des Betriebs und der Infrastruktur eingesetzt werden darf. Sie soll strafbare Handlungen gegen Personen und gegen die Infrastruktur der Transportunternehmen verhindern und die Aufklärung von strafbaren Handlungen ermöglichen oder unterstützen.

Überwachungsvarianten

Die Verordnung erfasst drei Varianten von Videoüberwachung. Bei der ersten Variante wird die Videokamera als elektronischer Rückspiegel eingesetzt: Die Bilder werden auf einen im Führerstand angebrachten Bildschirm übertragen. Diese Variante ermöglicht dem Fahrpersonal eine bessere Übersicht über das Geschehen im und am Fahrzeug sowie an der Haltestelle. Weil bei dieser Variante keine Daten bearbeitet werden, handelt es sich nicht um Datenbearbeitungen im Sinne von § 2 lit. f DSG. Da es für die betroffenen Personen nicht ersichtlich ist, ob eine Aufzeichnung und/oder Übertragung erfolgt, gilt gemäss Verordnung aus Transparenzgründen die Kennzeichnungspflicht auch für diese Einsatzart.

Bei der zweiten Variante werden die Bilder über einen gewissen Zeitraum aufgezeichnet und bei einem sicherheitsrelevanten Vorfall den zuständigen Behörden übergeben. Die Bilder können als Nachforschungs- und Beweismittel sichergestellt werden.

Bei der dritten Variante werden die Bilder aufgezeichnet und gleichzeitig an eine externe Zentrale übermittelt. Die Kamera kann mit einem SOS-Taster im überwachten Fahrzeug oder an der Hal-

testelle kombiniert werden. Wird das Signal ausgelöst, kann das Personal der Zentrale die übertragenen Bilder sofort analysieren und eine entsprechende Intervention auslösen. Zudem können die Bilder auch der nachträglichen Sicherstellung von Nachforschungs- und Beweismitteln dienen.

Gemäss dem Grundsatz der Verhältnismässigkeit (§ 4 Abs. 3 DSG) ist eine Videoüberwachung nur zulässig, wenn andere Massnahmen, die weniger stark in die persönliche Freiheit eingreifen, nicht oder nur mit einem viel höheren Aufwand zum Ziel führen. Untersagt ist die Überwachung des Geheimbereichs von Personen, wie Toilettenanlagen oder Garderoben. Unzulässig ist auch eine flächendeckende Überwachung mit Videokameras im Innen- und Aussenraum von öffentlichen Verkehrsmitteln. Grundsätzlich sollen nur Linien und Haltestellen überwacht werden, bei denen mit Vandalismus und Aggressionen gegenüber Fahrgästen und Personal zu rechnen ist.

Bewilligungspflicht

Damit Videokameras nicht undifferenziert eingesetzt werden, muss ein Einsatz bewilligt werden (§ 5 ff. der Verordnung). Der ZVV erteilt die Bewilligung auf Antrag der Verkehrsunternehmen. Die Bewilligung regelt die Rahmenbedingungen für Art und Umfang der Videoüberwachung, den Einsatzort, die Kennzeichnungspflicht, die Bewilligungsdauer und die Berichterstattung an den ZVV. Sie kann auch Einzelheiten regeln, wie die Anzahl der Videoanlagen oder Einschränkungen der Betriebszeiten. Aus Kosten-, betrieblichen oder technischen Gründen können Verkehrsunternehmen Einrichtung und Betrieb der Geräte sowie die Datenauswertung an Dritte übertragen. Eine solche Übertragung bedarf in jedem Fall der Ermächtigung durch den ZVV – auch dann, wenn die Übertragung an ein anderes Verkehrsunternehmen oder an einen Transportbeauftragten erfolgt.

Bedingungen für Auswertung

Die Verkehrsunternehmungen dürfen die Videoaufzeichnungen nur auswerten, wenn ein konkreter Vorfall gemeldet wird und die Auswertung zur Aufklärung des Sachverhaltes erforderlich ist (§§ 9–11 der Verordnung). Zwischen Meldung und Auswertung bedarf es eines unmittelbaren zeitlichen Zusammenhangs; die Auswertung muss deshalb spätestens am zweiten Werktag nach der Aufzeichnung angeordnet werden. Bei konkreten straf-, verwaltungs- oder zivilrechtlichen Vorfällen können die Daten bis zur Bekanntgabe an die zuständigen Behörden aufbewahrt werden. Ohne Auswertung sind die Daten 48 Stunden nach Ablauf der Auswertungsfrist zu löschen.

Auskunftspflicht

Das zur Videoüberwachung berechtigte Verkehrsunternehmen muss auf Anfrage allgemein über die Art der Aufzeichnung, der Datenspeicherung und der Datenauswertung informieren (§ 13 der Verordnung). Wer Auskunft über die Aufzeichnungen seiner Person verlangt (vgl. auch § 17 DSG), muss seine Anfrage in zeitlicher, örtlicher, persönlicher und sachlicher Hinsicht genügend bestimmen, damit eine Auskunftserteilung überhaupt möglich ist.

Anlagenschutz und Berichterstattung

Die Verkehrsunternehmen sind verpflichtet, die Videoüberwachungsanlagen und die Aufzeichnungen vor dem Zugriff unbefugter Personen zu schützen (§§ 12 und 15 der Verordnung). Die Einzelheiten, wie die Zugangsberechtigung, der Schutz vor unbefugtem Zugriff und die Weitergabe von Personendaten, müssen schriftlich geregelt werden. Die Verkehrsunternehmen müssen dem ZVV regelmässig Bericht über die Videoüberwachung erstatten. Mit dieser Wirksamkeitskontrolle wird gewährleistet, dass Videoüberwachungen eingestellt werden, wenn sie nicht mehr notwendig sind, oder dass alternative oder zusätzliche Massnahmen getroffen werden können, wenn die Zielsetzungen durch die Videoüberwachung nicht erreicht werden.

Fälle aus der Beratungstätigkeit

Ein Schwerpunkt der Tätigkeit des Datenschutzbeauftragten bildet die Beratungstätigkeit.

01. – 13. ***Die hier zusammengefassten Fälle sind ausführlich dargestellt im Anhang auf Seite 27 ff. und auf der Website des Datenschutzbeauftragten (www.datenschutz.ch).***

01. **Anspruch auf Berichtigung nach Strafverfahren**
Untersuchungsbehörden müssen den Austausch von Personendaten mit in- und ausländischen Behörden angemessen dokumentieren. Die betroffene Person muss die Möglichkeit haben, Verdächtigungen, die an Dritte weitergegeben wurden, sich später aber nicht bewahrheitet haben, berichtigen zu lassen.

02. **Fürsorge: Funktion bestimmt Einsicht**
Welches öffentliche Organ welche Einsicht in Fürsorgeakten der Sozialhilfebehörden erhält, hängt von seiner Funktion ab. Ob Haushaltsprüfung, Controlling oder verwaltungsrechtliche Aufsicht: Die Sozialbehörden müssen stets eine Interessenabwägung vornehmen.

03. **Einbürgerungen: Nur verhältnismässige Daten**
Im Rahmen eines Einbürgerungsverfahrens dürfen nur jene Daten einer einbürgerungswilligen Person veröffentlicht werden, die für die Einbürgerungsentscheidung wesentlich sind.

04. **Patientenbericht: Spital muss pseudonymisieren**
Werden Patientenberichte in einem Spital intern an die Personalabteilung weitergeleitet, müssen sie pseudonymisiert werden. An den Ombudsmann hingegen müssen sie grundsätzlich in der bestehenden, nicht pseudonymisierten Form weitergeleitet werden.

05. **Personendaten: Voraussetzung für Erhebung**
Werden Personendaten mit einem Fragebogen oder sonst systematisch erhoben, müssen Rechtsgrundlage und Zweck der Bearbeitung bekannt gegeben werden. Auch für die Datenbearbeitungen, deren Ergebnisse nicht publiziert werden, ist eine gesetzliche Grundlage notwendig.

06. **Denkmalschutzobjekte: Einsicht ins Inventar**
Das Einsichtsrecht Dritter in die Natur- und Heimatschutzinventare gemäss Planungs- und Baugesetz (PBG) beschränkt sich auf die Daten, die zur Erfüllung des Inventarzwecks unbedingt nötig sind.

07. **Anwendbares Datenschutzrecht für Stiftung**
In Bezug auf eine beitragsberechtigte privatrechtliche Stiftung muss in jedem Einzelfall separat abgeklärt werden, ob sie dem kantonalen oder dem eidgenössischen Datenschutzrecht untersteht.

08. **Fördermassnahmen: Datenerhebung erleichtert**
Bei Personendaten, die für nicht personenbezogene Zwecke – insbesondere in der Forschung, Planung und Statistik – bearbeitet werden, lässt das Datenschutzgesetz eine erleichterte Bearbeitung zu.

09. **Online-Angebot mit Einwilligung**
Die Gebäudeversicherung (GVZ) darf Banken, die im Hypothekargeschäft tätig sind, nur für jene Daten einen Online-Zugriff einrichten, für welche die Einwilligung der Gebäudeeigentümer vorliegt.

10. **Daten an die Sozialversicherung**
Personendaten sind in der Regel bei der betroffenen Person zu beschaffen. Verfügt die betroffene Person nicht über die verlangten Angaben, hat sie in einem zweiten Schritt dem bearbeitenden Organ eine Ermächtigung zur Datenbekanntgabe zu erteilen.

11. **Auskünfte der Einwohnerkontrolle**
Private Personen und Organisationen können der Einwohnerkontrolle Gesuche für die Bekanntgabe von Personendaten stellen. Die Voraussetzungen für die Bekanntgabe sind unterschiedlich.

12. **Keine Steuerdaten für Stadtmarketing**
Will das Steueramt Angaben, welche ihm zur Steuereinschätzung bekannt gegeben werden, zu einem anderen Zweck verwenden, braucht es eine entsprechende gesetzliche Grundlage oder eine vorgängige Einwilligung der betroffenen Person.

13. **Schützenswerte Interessen prüfen**
Kommt ein öffentliches Organ vorerst zum Schluss, dass eine Datenbekanntgabe zu erfolgen hat, muss es zudem die Umstände des Einzelfalles berücksichtigen und prüfen, ob offensichtlich schützenswerte Interessen des Betroffenen eine Einschränkung verlangen.

Informationssicherheit vielfach mangelhaft

Der Datenschutzbeauftragte fokussierte 2006 seine Kontrolltätigkeit auf Gemeinden und Stellen in einem komplexen Umfeld. Die Datenschutzreviews zeigten erneut kritische Defizite auf der strategischen und der operativen Ebene auf.

Der Datenschutzbeauftragte kontrollierte im Jahr 2006 insbesondere öffentliche Organe in einem komplexen Umfeld sowie Gemeinden. Die Prüfungszielsetzungen umfassten folgende Aspekte:

- abgenommene IT-Sicherheitsstrategie oder -Sicherheitsleitlinie
- zugewiesene Verantwortung für IT-Sicherheit und Datenschutz
- aktuelle Weisungen für Benützende und Betriebsdokumentationen für Betreibende
- richtige Verwendung von Passwörtern und deren technische Umsetzung
- korrekte Berechtigungs- und Rollenkonzepte (Zugriffskonzepte)
- sichere Anbindung von Netzwerken
- aktuelle Anleitungen für den Umgang mit mobilen Geräten (wie Notebooks oder Personal Digital Assistants, PDA)
- sicherer Betrieb von Web Services unter Berücksichtigung der Rahmenbedingungen («Privacy Policy»)

Die wichtigsten Empfehlungen des Datenschutzbeauftragten blieben 2006 unverändert (siehe Tätigkeitsbericht Nr. 11 [2005], S. 32, Statistik 2). Die Umsetzung von minimalen Massnahmen in den geprüften Stellen erfolgt meistens zaghaft. Ein ausreichender und angemessener Schutz der Daten bleibt eine grosse Herausforderung. Erreicht werden kann er nur durch eine Prioritätenverschiebung in den geprüften Stellen. Eine angemessene Sicherheitskultur muss sogar in den Stellen, die zum Teil bereits über gute Ansätze bei der Umsetzung ihrer Massnahmenpläne verfügen, erst etabliert oder weiter ausgebaut werden.

Schwerpunkte bei Gemeinden

Der Datenschutzreview zeigt bei den Gemeinden folgende problematische Bereiche:

- Know-how- und Informationsdefizite besonders im Bereich IT-Sicherheit
- Die Abhängigkeit von den externen Dienstleistenden kann die Beurteilung der Situation im Sicherheitsbereich erschweren oder verunmöglichen. Langjährige Zusammenarbeit garantiert keinen sicheren Betrieb von Hard- und Software.

Wie bereits früher festgestellt ist das Massnahmenniveau der geprüften Gemeinden deutlich tiefer als der Durchschnitt der übrigen öffentlichen Organe (siehe Tätigkeitsbericht Nr. 11 [2005], S. 32). Ein grosser Nachholbedarf besteht bei folgenden grundlegenden Themen:

- fehlender Auftrag für Informationssicherheit aufgrund einer fehlenden Sicherheitsstrategie oder -leitlinie
- nicht zugewiesene Verantwortlichkeiten
- Einzelmassnahmen ohne übergreifendes Zugriffskonzept

Dieser Nachholbedarf lässt auf ein weiterhin mangelndes Verständnis für diese Themen schliessen, wodurch die Bereitstellung der notwendigen Ressourcen weiter verzögert wird.

Geprüfte Amtsstellen

In den geprüften Amtsstellen und Fachhochschulen sind zwar Massnahmenkataloge vorhanden, doch die Umsetzung erfolgt erst teilweise: Die Wirksamkeit der Massnahmen wird nicht überprüft. Mit der kontinuierlichen Priorisierung (wie die «Siegelstufen» des neuen Grundschutzkatalogs) ist noch nicht begonnen worden. Das Vorgehen bei der Umsetzung erfolgt nicht gemäss Standards wie zum Beispiel 100-2 des BSI. Als Gründe werden meistens fehlende Ressourcen oder die zu komplexe IT-Umgebung genannt. Entsprechend sind die Anforderungen für IT-Sicherheit in den Projekten und im Betrieb meist nicht homogen, und die getroffenen Massnahmen wirken teilweise zufällig.

Managementsysteme

Komplexe Umgebungen brauchen Managementsysteme für IT-Sicherheitsmassnahmen. Alle verantwortlichen Stellen verfügen über die entsprechenden Stan-

dards für Aufbau und Inhalt eines entsprechenden Managementsystems (ISO/IEC 27000-1 oder BSI 100-1). Nach der Aufbauphase kann die Wirksamkeit im Rahmen einer Zertifizierung bestätigt werden. Das neue Informations- und Datenschutzgesetz (IDG) ermöglicht ab 1. Januar 2008, die Managementsysteme nach Standards zu prüfen und zu zertifizieren.

Sensibilisierung für Sicherheit

Der Datenschutzbeauftragte engagiert sich schon länger im Bereich der Sicherheit von Netzwerken, mobilen Arbeitsplätzen und Geräten (siehe Tätigkeitsbericht Nr. 11 [2005], S. 31). Die Arbeitsgruppe ZH171 hat sich unter Beteiligung des Datenschutzbeauftragten mit dem Thema Netzwerksicherheit befasst. Zur Arbeitsgruppe gehören die Interessengemeinschaft IG EDV als Vertreter der zürcherischen Gemeinden, die Vertreter des Kantonalen IT-Teams KITT sowie Vertreter von grossen Städten. Schwerpunkte waren die Network Security Policy des Gemeindenetzwerks und die Klärung von zahlreichen Detailaspekten zum logischen Netz der Gemeinden innerhalb des kantonalen Gesamtnetzes LEUnet.

Einheitliche Standards und Methoden

Der Datenschutzbeauftragte hat zusammen mit der Finanzkontrolle und den Revisionsdiensten des Gemeindeamts im Sommer 2006 die Arbeitsgruppe «Methoden und Standards» gebildet. Deren Zielsetzungen sind die Erarbeitung sowohl eines einheitlichen Prüfungsvorgehens (Methode) als auch eines einheitlichen Prüfungsmassstabs und einheitlicher Massnahmenkataloge (Standards). Um die Ressourcen der prüfenden und der geprüften Stellen optimal einsetzen zu können, sollen die Prüfungen zwischen den Prüfstellen koordiniert werden. Der Datenschutzreview wird in Umfang und Vorgehen an das vereinbarte Niveau angepasst, damit die Resultate von den anderen Prüfstellen direkt weiterverwendet werden können. Verstärkt berücksichtigt werden international anerkannte Methoden und Standards, wie die Standards 100-1 bis 100-3 des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Grundschutzkatalogs.

Die Arbeitsgruppe «Methoden und Standards» hat sich intensiv mit der Klassifikation der Stellen, dem Minimalstandard bei Massnahmenplänen und dem Prüfungsmassstab auseinandergesetzt. Da die Beratungsleistungen von den Prüfungsempfehlungen und vom Prüfungsmassstab direkt abhängen, hat der Datenschutzbeauftragte für eine effiziente Beratung und als Mittel zur Selbsthilfe eine mögliche Vorgehensweise sowie entsprechende Hilfsmittel für die Umsetzung von Informatiksicherheitsmassnahmen für kleine und mittlere Stellen zusammengestellt. Diese wiederum fliessen auch wieder als Anforderung in den Datenschutzreview ein. Kernpunkt des Projekts ist, in Anlehnung an den BSI-Standard 100-2, ein möglichst einfaches Verfahren, das auch von IT-Verantwortlichen ohne grosses Know-how und mit bescheidenen Ressourcen durchgeführt werden kann. Die Arbeitsgruppe «Methoden und Standards» liefert dazu wertvolle Hinweise in den Bereichen Klassifizierung und Minimalstandards. Diskutiert wird zudem ein Standard-Tool für die geprüften Stellen, das sowohl die Modellierung der Stelle als auch die Erstellung und Verwaltung der Massnahmenkataloge vereinfacht. Gleichzeitig soll es den Datenaustausch bei der Prüfung und bei der Beratung der Stellen durch den Datenschutzbeauftragten verbessern.

Daten über Hundehalter

Aus datenschutzrechtlicher Sicht sind die Personendaten des Hundehalters relevant – nicht aber die Daten seines Hundes.

Im Zusammenhang mit der Einführung des Leinen- und Maulkorbzwanges für bestimmte Hunderassen (§ 7a Hundeverordnung) sowie der Totalrevision des Hundegesetzes wurde der Datenschutzbeauftragte für verschiedene Stellungnahmen angefragt.

Hundehalter mit Hunden, die unter die Leinen- und Maulkorbpflicht fallen, können eine Ausnahmebewilligung erlangen. Sie müssen dazu einen detaillierten Fragebogen ausfüllen, der auch Daten zu ihrer Person enthält. Zuständig für das Bewilligungsverfahren ist das Veterinäramt.

Nach Einschaltung des Datenschutzbeauftragten änderte das Veterinäramt aus Gründen der Verhältnismässigkeit (§ 4 Abs. 3 DSG) den Fragebogen ab: Die Angaben über Beruf und Arbeitgeber des Hundehalters sowie die Nennung der Personen aus dem Umfeld des Hundes sind nun nicht mehr zu erheben.

Im Zuge eines weiteren Ausnahmebewilligungsverfahrens musste ein Wesenstest mit dem Hund absolviert werden. Gestützt auf § 7a der Hundeverordnung wurde der Wesenstest auf Video festgehalten. Weil auf dem Video nicht nur der Hund, sondern auch die Halterin erkennbar ist, handelt es sich bei der Aufzeichnung um eine Personenbearbeitung im Sinne des DSG. Die datenschutzrechtlichen Bestimmungen müssen entsprechend eingehalten werden.

Im Kanton Zürich wird die Registrierung der Daten über Hundehaltungen an die Anis AG ausgelagert. Voraussetzung dafür ist § 13 DSG: Beauftragt ein öffentliches Organ einen Dritten mit dem Bearbeiten von Personendaten, ist der Datenschutz durch Auflagen, Vereinbarungen oder auf andere Weise sicherzustellen. Ohne ausdrückliche Ermächtigung dürfen Daten ausschliesslich für das auftraggebende Organ verwendet und nur diesem bekannt gegeben werden. Die Verantwortung liegt jedoch weiterhin beim öffentlichen Organ (§ 6 DSG).

Der Kanton Zürich hat mit der Anis AG eine Vereinbarung abgeschlossen, welche die Einzelheiten der Zusammenarbeit regelt. Im Rahmen der Verhältnismässigkeit dürfen nur Personendaten bearbeitet werden, welche für die Aufgabenerfüllung geeignet und erforderlich sind.

Lernprogramm Datenschutz

Der Datenschutzbeauftragte stellt auf seiner Website ein umfassendes Lernprogramm zum Datenschutz zur Verfügung. Und stösst damit auf grosses Interesse – sowohl verwaltungsintern als auch in der Öffentlichkeit.

Datenbearbeitungen und somit auch der Datenschutz gehören zum Alltag von unzähligen Angestellten der öffentlichen Verwaltung. Um sie für die umfassende Datenschutz-Thematik zu sensibilisieren und ihnen den praktischen Umgang mit dem Datenschutzgesetz zu erläutern, hat der Datenschutzbeauftragte ein interaktives Lernprogramm entwickelt (siehe www.datenschutz.ch/wbt/datenschutz). Es erklärt die Grundprinzipien des kantonalen Datenschutzgesetzes und veranschaulicht sie mit zahlreichen Praxisbeispielen. In einem ersten Kapitel werden die rechtlichen Grundlagen auf verständliche Weise erläutert. Das zweite Kapitel enthält zahlreiche Fallbeispiele aus unterschiedlichen Verwaltungsbereichen und ermöglicht so, das Gelernte an konkreten Praxisfällen zu üben. Das Programm gibt aber auch zahlreiche Hinweise auf weiterführende Informationen, welche sich auf der Website des Datenschutzbeauftragten finden. Damit sind auch die aktuellen Informationen ständig im Lernprogramm abrufbar. Insbesondere eine generelle Einführung in das Thema des Datenschutzes ermöglicht es Personen, die nicht oder nur selten in ihrer beruflichen Praxis mit dem Datenschutz in Berührung kamen, einen ersten Überblick zu finden. Das Gelernte kann abschliessend in einem Quiz überprüft werden. Es ist möglich, das Lernprogramm in verschiedenen Schritten zu absolvieren; insgesamt beträgt der Aufwand je nach Vorkenntnissen aber nur wenige Stunden.

Das Lernprogramm zum Datenschutz richtet sich auch an alle Interessierten ausserhalb der öffentlichen Verwaltung, die mehr über den Datenschutz erfahren wollen und sich über ihre Rechte bei Datenbearbeitungen informieren möchten.

Damit entspricht das Lernprogramm dem wachsenden Bedürfnis nach konkreten Informationen zum Datenschutz. Bereits in den ersten Monaten haben mehrere hundert Personen das Lernprogramm absolviert. Auch zahlreiche positive Rückmeldungen von Absolvierenden des Lernprogramms bestätigen, dass die Datenschutzthematik und diese Art der Vertiefung einem eigentlichen Bedürfnis entsprechen.

Schutz der Privatheit bleibt im Fokus

Die Geschäftsprüfungskommission des Kantonsrats (GPK) lässt sich regelmässig über die Schwerpunkte der Tätigkeit des Datenschutzbeauftragten informieren. Im Rahmen dieses Dialoges diskutiert sie mit dem Datenschutzbeauftragten auch datenschutzrechtliche Fragestellungen aus den verschiedensten Bereichen.

Die gesellschaftlichen und technologischen Entwicklungen stellen den Schutz der Privatheit der Bürgerinnen und Bürger stets vor neue Herausforderungen. Von zunehmender Bedeutung sind der Umgang mit Patienteninformationen und das Bearbeiten von Personendaten im Bereich der polizeilichen Ermittlung. Generell muss der Zugang respektive Nichtzugang zu Informationen umfassend betrachtet werden – so wie dies das neue Informations- und Datenschutzgesetz (IDG) vorsieht.

Neue Technologien bringen neue Risiken für den Datenschutz. Auch die Verwaltung setzt in allen Bereichen auf modernste Technologien und Datenbearbeitungsmethoden wie Data Warehousing und Data Mining. Häufig sind die Risiken dabei nur ungenügend abgedeckt, und entsprechende Rechtsgrundlagen – wie beispielsweise im Bereich der Raumdaten – fehlen.

Verschiedene Themen betrafen unter anderem die Interessenabwägung im Einzelfall zwischen den Informationsbedürfnissen der Verwaltung und der Privatsphäre der betroffenen Person. In § 14 Abs. 3 IDG ist neu für den Bereich der hängigen Verfahren vorgesehen, dass das öffentliche Organ bei falschen Meldungen oder im Sinne von Berichtigungen informieren kann. Des Weiteren gab der zunehmende Einsatz von biometrischen Verfahren bei Zugangskontrollen oder bei Überprüfungen zu Fragen Anlass. Der Datenschutzbeauftragte hat sich hierzu bereits verschiedentlich geäussert. Nun geht es auch darum, dieses System in der Praxis zu überprüfen. Mangels entsprechender Ressourcen konnte dies bisher nicht erfolgen.

Die GPK äusserte sich dahingehend, dass sie die Informationssysteme im Bereich der Raumdaten, deren ungenügenden rechtlichen Grundlagen der Datenschutzbeauftragte seit langem bemängelt, einer näheren Prüfung unterziehen werde.

Der regelmässige Austausch mit der GPK zeigt, dass die Herausforderungen für den Schutz der Privatheit der Bürgerinnen und Bürger nach wie vor gross sind. Neue Projekte der Verwaltung bringen immer wieder neue Anforderungen, wobei dem Datenschutz jeweils ein unterschiedlicher Stellenwert zugewiesen wird. Die laufende Beratung, eine regelmässige Kontrolle und die Information über die Anliegen des Datenschutzes sind dabei die wichtigsten Elemente für einen nachhaltigen Datenschutz in der Verwaltung.

Plattform für Privatheit und Sicherheit

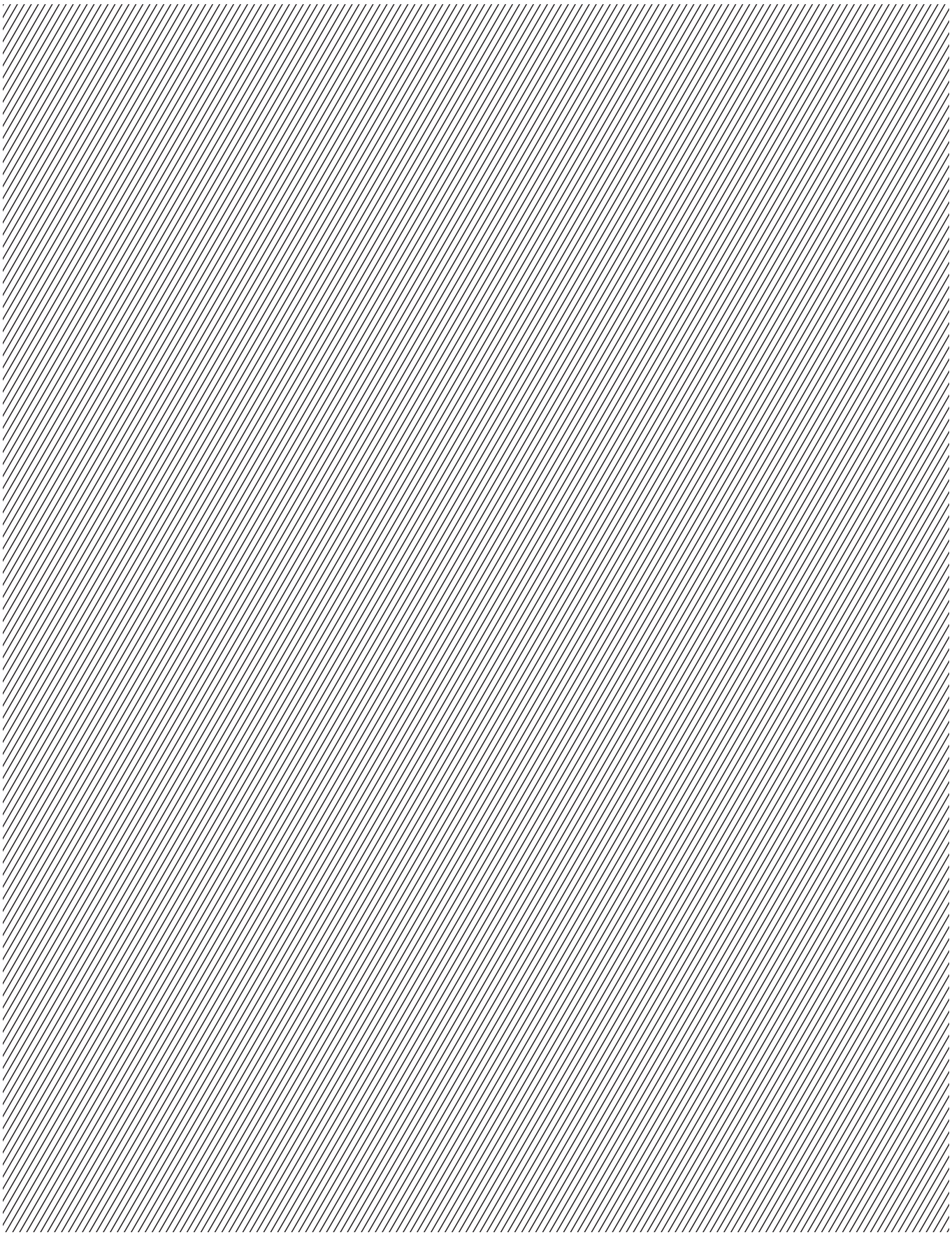
Das Symposium on Privacy and Security (SPS) widmete sich 2006 der Verselbständigung des Computers – einem technologischen Trend mit weitreichenden Folgen für den Datenschutz. Das Symposium wird von der Stiftung für Datenschutz und Informationssicherheit gemeinsam mit dem Swiss Re Centre for Global Dialogue organisiert.

Das SPS entstand aus einer Zusammenarbeit des Datenschutzbeauftragten mit der ETH Zürich. Seit 1996 bietet es eine Plattform, auf der Wirtschaft, Politik, Verwaltung und Wissenschaft Fragen zu Privatheit und Sicherheit mit ihren rechtlichen, technischen, wirtschaftlichen, politischen und ethischen Aspekten interdisziplinär behandeln können. Das Symposium 2006 widmete sich der Verselbständigung des Computers.

Fortschritte in der Miniaturisierung der Computer, in der Sensor- und in der Kommunikationstechnologie sowie in den Materialwissenschaften führen dazu, dass die Computer in Alltagsgegenständen – im Pullover, in der Eintrittskarte, in Verpackungen oder in Fahrzeugen – unsichtbar integriert werden. Sie nehmen Umwelt und Personen immer feinfühliger wahr, können sich selbständig miteinander vernetzen und das, was sie wahrgenommen und getan haben, auch in Erinnerung behalten. In zahlreichen Lebens- und Geschäftsbereichen bieten sich dafür sinnvolle Anwendungen. Es entsteht das Zukunftsbild einer angenehmen, unauffälligen Technologieunterstützung im Alltag, von mehr Sicherheit im Verkehr und in der Gesellschaft, von mehr Autonomie der Patientinnen und Patienten.

Gleichzeitig rücken offene Fragen und Risiken ins Blickfeld. Es wird etwa geltend gemacht, bei Pervasive Computing seien Haftungsfragen ungelöst (oder sogar unlösbar). Es wird eingewendet, die informationelle Selbstbestimmung gehe vollends verloren und das Datenschutzrecht versage angesichts der allumfassenden Datenbearbeitungen. Es wird vermutet, die Informationssicherheit sei angesichts der Vernetzung nicht zu gewährleisten. Und schliesslich wird erkennbar, dass die Abhängigkeit von Infrastruktur zur kritischen Grösse werden kann.

Anhand von ausgewählten Anwendungsbeispielen beleuchtete das SPS 2006 die Chancen und Risiken dieser neuen Technologien und leistete damit einen wichtigen Beitrag für künftige Diskussionen in diesem Bereich.



Fälle aus der Beratungstätigkeit
Anhang

Titel: Anspruch auf Berichtigung nach Strafverfahren
URL: http://www.datenschutz.ch/themen/1299.php
Datum: 17.07.2007

01.

Anspruch auf Berichtigung nach Strafverfahren

Untersuchungsbehörden müssen den Austausch von Personendaten mit in- und ausländischen Behörden angemessen dokumentieren. Die betroffene Person muss die Möglichkeit haben, Verdächtigungen, die an Dritte weitergegeben wurden, sich später aber nicht bewahrheitet haben, berichtigen zu lassen.

Strafverfolgungsbehörden tauschen im Rahmen ihrer Ermittlungen Personendaten mit in- und ausländischen Behörden aus. Zu diesen Daten gehören auch Verdächtigungen und Mutmassungen, die sich später als unrichtig erweisen. Aus den Untersuchungsakten geht oft nicht hervor, mit welchen in- und ausländischen Behörden im Laufe des Verfahrens welche Personendaten ausgetauscht wurden. Eine Richtigstellung von allfälligen Verdächtigungen und Mutmassungen gegenüber Dritten unterbleibt.

Der Datenschutzbeauftragte beleuchtete anlässlich eines konkreten Falles die Verantwortlichkeiten und den Anwendungsbereich des Datenschutzgesetzes.

Das Datenschutzgesetz gilt für das Bearbeiten von Personendaten durch öffentliche Organe; es gilt jedoch nicht in hängigen Verfahren der Strafrechtspflege (§ 3 Abs. 1 und Abs. 2 lit. b DSG). Für den Datenschutz – und damit für die Wahrung der Rechte der betroffenen Person – ist das Organ verantwortlich, das die Personendaten im Rahmen seiner Aufgaben bearbeitet oder bearbeiten lässt (§ 6 Abs. 1 DSG; § 17 ff. DSG). Dies bedeutet:

- Solange die Polizei zur vorbeugenden Verbrechensbekämpfung ermittelt und der Untersuchungsbehörde noch keinen Bericht über ihre Ermittlungen erstattet hat (§ 22 Abs. 1 StPO), ist die Polizei verantwortliches Organ im Sinne von § 6 Abs. 1 DSG. Für die entsprechenden Daten ist zu diesem Zeitpunkt das Datenschutzgesetz anwendbar (§ 3 Abs. 1 DSG).
- Sobald die Polizei der Untersuchungsbehörde Bericht im Sinne von § 22 Abs. 1 StPO erstattet hat, wird die Untersuchungsbehörde für den berichteten Bereich verantwortliches Organ (§ 25 Abs. 1 StPO, § 6 Abs. 1 DSG). Dies gilt auch für die Datenbearbeitung der Polizei, wenn sie die Untersuchungsbehörden unterstützt. Für die entsprechenden Daten ist zu diesem Zeitpunkt das Datenschutzgesetz anwendbar (§ 3 Abs. 1 DSG).
- Mit der Eröffnung einer Untersuchung im Sinne von § 22 Abs. 4 StPO werden die Prozessgesetze für alle im betreffenden Strafverfahren durch die Untersuchungsbehörde und die sie unterstützende Polizei bearbeiteten Personendaten anwendbar (§ 3 Abs. 2 lit. b DSG).
- Nach der rechtskräftigen Erledigung gelten nicht mehr die Prozessgesetze, sondern das Datenschutzgesetz – und zwar für die polizeilichen und untersuchungsbehördlichen Daten. Die skizzierte Verantwortlichkeit im Sinne von § 6 Abs. 1 DSG bleibt jedoch bestehen.

Auskunfts- und Berichtigungsrecht

Gemäss Datenschutzgesetz kann jede Person Auskunft darüber verlangen, welche Daten ein verantwortliches Organ in seinen Datensammlungen bearbeitet und an welche Stellen Daten weitergegeben worden sind (§ 17 DSG). Entsprechend müssen die Strafverfolgungsbehörden sicherstellen, dass alle prozessualen Vorgänge festgehalten und in der Strafakte dokumentiert sind: Die schriftliche Weitergabe von Daten muss mit einer Kopie der schriftlichen Mitteilung in

den Akten dokumentiert werden, die mündliche Weitergabe von Daten mit einem entsprechenden Aktenvermerk.

Personendaten müssen richtig und gemäss Bearbeitungszweck vollständig sein (§ 4 Abs. 2 DSG); nicht mehr benötigte Daten sind zu vernichten. Wer ein schützenswertes Interesse hat, kann somit vom verantwortlichen Organ verlangen, dass es Daten berichtigt oder vernichtet (§ 19 Abs. 2 lit. a DSG). Kann weder die Richtigkeit noch die Unrichtigkeit von Daten bewiesen werden, bringt das verantwortliche Organ bei den Daten einen entsprechenden Vermerk an (§ 19 Abs. 3 DSG).

Dritte, die bereits Daten erhalten haben, die sich nachträglich als unrichtig erwiesen haben, müssen auch die Berichtigungen erhalten. Eine Frage des Einzelfalles ist hingegen, ob ein Anspruch darauf besteht, dass die in- und ausländischen Stellen, denen im Verlaufe des Verfahrens Personendaten übermittelt worden sind, über die Einstellung des Verfahrens und/oder über einen Freispruch zu informieren sind. Soweit dem Betroffenen Nachteile dadurch entstehen können, dass die in- und ausländischen Stellen nicht darüber informiert worden sind, dass sich der ursprüngliche Straftatverdacht nicht bestätigt hat, wird man ein schützenswertes Interesse an einer Berichtigung bejahen müssen. Die betroffene Person hat einen Anspruch darauf, dass Strafverfolgungsbehörden bei nachfolgenden Entscheiden beachten, dass sich die ursprüngliche Verdächtigung nicht bestätigt hat oder der Verdacht widerlegt wurde. Soweit die Daten nicht nur an die Strafverfolgungsbehörden, sondern auch an andere Stellen weitergegeben worden sind, darf die betroffene Person keine beruflichen oder sonstigen Nachteile dadurch erleiden, dass sie weiterhin zu Unrecht als eine straftatverdächtige Person geführt und entsprechend behandelt wird.

Ein vom Datenschutzbeauftragten in Auftrag gegebenes Gutachten zu datenschutzrechtlichen Fragestellungen in Bezug auf den Austausch von Personendaten mit in- und ausländischen Behörden durch die Strafverfolgungsbehörden des Kantons Zürich wurde von Prof. Dr. Wolfgang Wohlers, Universität Zürich, erstellt und bestätigt diese Darlegungen. Die Schlussfolgerungen wurden auch den Untersuchungsbehörden zur Verfügung gestellt. In Zusammenarbeit mit dem Datenschutzbeauftragten sollen die entsprechenden Weisungen für die Untersuchungsführung ergänzt werden.

Titel: Fürsorge: Funktion bestimmt Einsicht
URL: http://www.datenschutz.ch/themen/1300.php
Datum: 17.07.2007

02.

Fürsorge: Funktion bestimmt Einsicht

Welches öffentliche Organ welche Einsicht in Fürsorgeakten der Sozialhilfebehörden erhält, hängt von seiner Funktion ab. Ob Haushaltsprüfung, Controlling oder verwaltungsrechtliche Aufsicht: Die Sozialbehörden müssen stets eine Interessenabwägung vornehmen.

Der Datenschutzbeauftragte wurde von verschiedenen Seiten gebeten, datenschutzrechtliche Fragestellungen in den Bereichen Haushaltsprüfung, Controlling und Verwaltungsaufsicht im Fürsorgebereich zu beantworten.

Fürsorgedaten sind besonders schützenswerte Personendaten (§ 2 lit. d Ziff. 3 DSG). Für die Bearbeitung dieser Daten ist eine klare gesetzliche Grundlage nötig, oder die Datenbearbeitung muss zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich sein (§ 5 lit. a und b DSG). Zudem ist der Grundsatz der Verhältnismässigkeit (§ 4 Abs. 3 DSG) zu beachten und die Bekanntgabe durch die Fürsorgebehörde zu verweigern, einzuschränken oder mit Auflagen zu verbinden, wenn wesentliche öffentliche Interessen oder offensichtlich schützenswerte Interessen einer betroffenen Person es verlangen (§ 10 lit. a DSG).

Für die Offenlegung von Fürsorgedaten ist die Aufgabenstellung der jeweiligen Prüfungsart entscheidend. Es wird dabei zwischen Haushaltsprüfung, Controlling und verwaltungsrechtlicher Aufsicht unterschieden:

a) Haushaltsprüfung

Jede politische Gemeinde bestellt eine Rechnungsprüfungskommission (RPK) von mindestens fünf Mitgliedern für die Überwachung des Finanzhaushalts (§ 83a Abs. 1 Gemeindegesetz). Das Kontrollorgan prüft, ob die Ausgaben rechtlich zulässig, die Einnahmen vollständig, das Kassen- und Rechnungswesens rechnerisch richtig und die Anträge mit finanzieller Tragweite wirtschaftlich angemessen sind. Dazu erhalten die Kontrollorgane Einsicht in Fürsorgeakten. Sie haben jedoch nur Anspruch auf Einsicht in Informationen, welche zur Aufgabenerfüllung geeignet und erforderlich sind (Verhältnismässigkeit, § 4 Abs. 3 DSG). Vorgängig müssen die Sozialbehörden eine Interessenabwägung zwischen den öffentlichen Interessen an der Haushaltsprüfung und den schutzwürdigen Interessen der Fürsorgeempfänger vornehmen (§ 10 DSG). So dürfen Haushaltsprüfungsorgane keine Einsicht in Akten nehmen, die den höchst persönlichen Bereich von Personen betreffen, wie detaillierte Begründungen von Fürsorgeentscheiden oder Fallakten mit detaillierten Angaben.

b) Controlling

Ein Controlling stellt die Planung, Koordination und Steuerung der Verwaltungstätigkeit sicher und dient der Effizienzkontrolle. Die Gemeinde regelt in einem Erlass, wer die Controllingfunktion übernimmt. Das Controlling erfordert eine umfassendere Akteneinsicht durch die zuständige Instanz als eine Haushaltsprüfung. Es bedarf jedoch einer präzisen Aufgabenumschreibung, um beurteilen zu können, ob eine Einsicht in besonders schützenswerte Personendaten gerechtfertigt ist. Allgemein kann davon ausgegangen werden, dass eine solche Einsicht in der Regel weder geeignet noch erforderlich ist, da keine materielle Prüfung von konkreten Einzelfällen erfolgt. Die Einsicht kann – falls überhaupt – nur im Einzelfall nach einer entsprechenden Güterabwägung (§ 10 DSG) bejaht werden.

c) Verwaltungsrechtliche Aufsicht

Die verwaltungsrechtliche Aufsicht erfordert den weitesten Umfang der Einsicht. Der Bezirksrat beaufsichtigt die Fürsorgebehörden (§ 8 Sozialhilfegesetz). Die Aufsicht richtet sich nach §§ 141 ff. Gemeindegesetz. Die Akteneinsicht ist ein wesentliches Mittel der Aufsicht. Insofern genügen entsprechende gesetzliche Bestimmungen im Sozialhilfe- und Gemeindegesetz den Anforderungen von § 5 DSG. Der Bezirksrat darf deshalb Einsicht in die Fallakten nehmen, soweit die Datenbekanntgaben für die Erfüllung seiner Aufsichtsaufgaben geeignet und erforderlich sind (§ 4 Abs. 3 DSG). Die Aufsichtsbehörde darf beispielsweise beim Verdacht auf ungerechtfertigte Sozialbezüge eine materielle Prüfung der Akten durchführen. Doch auch für die verwaltungsrechtliche Aufsicht müssen die Sozialbehörden eine Interessenabwägung vornehmen (§ 10 DSG). Da das öffentliche Interesse an einer gut funktionierenden Verwaltungsaufsicht erheblich ist, ist ein Ausschluss der Einsicht in einen Fürsorgefall nur in ganz seltenen Fällen gerechtfertigt. Ein Schutzinteresse des Fürsorgeempfängers kann sich allenfalls auch nur auf ein einzelnes Aktenstück beziehen.

Derzeit läuft ein Gesetzgebungsprojekt, das die Prüfung der Finanzhaushalte der Gemeinden und anderen Organisationen des öffentlichen Rechts durch unabhängige und fachliche Organe (vgl. Art. 129 Abs. 4 KV) auf Gesetzesstufe umsetzen wird. Die RPK der Gemeinden werden in der bisherigen Form abgelöst und analog der Finanzkontrolle auf kantonaler Ebene durch Organe, die voraussichtlich mit einem erweiterten Aufgabenbereich und entsprechenden Einsichtsbefugnissen betraut werden, ersetzt.

Auch in den neu zu schaffenden Rechtsgrundlagen werden nebst der notwendigen klaren gesetzlichen Grundlage gemäss § 5 DSG das Verhältnismässigkeitsprinzip (§ 4 Abs. 3 DSG) sowie die Güterabwägung gemäss § 10 DSG im Einzelfall ausschlaggebend sein für die Beurteilung, ob eine Einsicht gewährt werden kann. Der Datenschutzbeauftragte verweist diesbezüglich auf die bestehenden Bestimmungen in § 25 Abs. 2 Finanzkontrollgesetz.

Titel: Einbürgerungen: Nur verhältnismässige Daten
URL: http://www.datenschutz.ch/themen/1301.php
Datum: 17.07.2007

03.

Einbürgerungen: Nur verhältnismässige Daten

Im Rahmen eines Einbürgerungsverfahrens dürfen nur jene Daten einer einbürgerungswilligen Person veröffentlicht werden, die für die Einbürgerungsentscheidung wesentlich sind.

Im Rahmen eines Einbürgerungsverfahrens wurden die folgenden Daten einer einbürgerungswilligen Person im Weisungsheft zur ordentlichen Gemeindeversammlung veröffentlicht: Angaben zum steuerlichen Einkommen und Vermögen, Angaben über den Arbeitgeber und die Anstellung sowie Angaben zu den Betreibungsregisterauszügen. Das Weisungsheft wurde an alle Stimmberechtigten (Bürgergemeinde, politische Gemeinde, Primarschulgemeinde sowie reformierte Kirchgemeinde) verschickt.

Die Datenbekanntgabe im Einbürgerungsverfahren muss dem Kriterium der Verhältnismässigkeit (§ 4 Abs. 3 DSG) genügen. Das Material, das die Stimmberechtigten erhalten, darf nur jene Daten enthalten, die nötig sind, um die Kandidatinnen und Kandidaten zu identifizieren und die Anträge bekannt zu geben: Dies sind Name, Vorname, Geburtsjahr, Adresse und Herkunftsland. Zusätzliche Angaben sind weder geeignet noch erforderlich und haben somit zu unterbleiben.

Der Informationsbedarf der stimmberechtigten Bürgerinnen und Bürger ist ausreichend gedeckt, wenn sie Gelegenheit haben, die für ihren Entscheid relevanten Akten vor der Abstimmung in der Gemeindekanzlei einzusehen. Doch selbst dort dürfen keine vollständigen Akten über eine einbürgerungswillige Person aufliegen, sondern nur eine Zusammenfassung jener Fakten, die für die Entscheidung über die Einbürgerung wesentlich sind. Die Einkommens- und Vermögenssituation gehört nicht dazu.

Bearbeitet ein öffentliches Organ Daten unrechtmässig, kann die betroffene Person, die ein schützenswertes Interesse hat, verlangen, dass die unerlaubte Datenbearbeitung in Zukunft unterlassen wird. Sie kann zudem verlangen, dass festgestellt wird, dass die Daten unerlaubterweise bearbeitet wurden, und dass die Folgen daraus beseitigt werden. Dazu kann der Entscheid oder die Berichtigung veröffentlicht oder Dritten mitgeteilt werden (§19 DSG).

Titel: Patientenbericht: Spital muss pseudonymisieren
URL: http://www.datenschutz.ch/themen/1302.php
Datum: 17.07.2007

04.

Patientenbericht: Spital muss pseudonymisieren

Werden Patientenberichte in einem Spital intern an die Personalabteilung weitergeleitet, müssen sie pseudonymisiert werden. An den Ombudsmann hingegen müssen sie grundsätzlich in der bestehenden, nicht pseudonymisierten Form weitergeleitet werden.

Im Rahmen eines Personalkonflikts in einem öffentlichen Spital wurden die Personalakten mehrerer Sekretärinnen sowohl intern an die Personalabteilung als auch von der Personalabteilung an den Ombudsmann weitergeleitet. In dem Dossier einer Sekretärin befanden sich zahlreiche Patientenberichte – inklusive Namen und Geburtsdaten der Patienten. Die Patientenberichte sollten die Tippfehler der Sekretärin belegen und dadurch deren Entlassung begründen.

Für die Weiterleitung der Patientenberichte des Spitals an die Personalabteilung war keine klare gesetzliche Grundlage ersichtlich. Um die Tippfehler zu dokumentieren und nachweisen zu können, dass sie von einer bestimmten Person stammen, hätte es im konkreten Fall ausgereicht, der Personalabteilung pseudonymisierte Patientenberichte zuzustellen. Die Datenbekanntgabe erschien somit als unverhältnismässig. Zudem wäre die Personalabteilung nach Empfang der Berichte verpflichtet gewesen, diese in pseudonymisierter Form aufzubewahren und die personenbezogenen Patientendaten zu vernichten (§ 4 Abs. 3 DSG).

Für die Datenbekanntgabe durch die Personalabteilung an den Ombudsmann gelten die Bestimmungen der §§ 89 Abs. 1 und 92 Abs. 2 VRG: Behörden, mit denen sich der Ombudsmann in einem bestimmten Fall befasst, sind dem Ombudsmann gegenüber zur Auskunft und zur Vorlage der Akten verpflichtet. Da die Personalabteilung die Patientenberichte in nicht pseudonymisierter Form aufbewahrt hatte, war sie aufgrund von § 92 VRG grundsätzlich dazu verpflichtet, dem Ombudsmann die verlangten Akten in der bestehenden Form herauszugeben. Die Personalabteilung hätte sich allerdings auf ein offensichtlich schützenswertes Interesse einer betroffenen Person berufen und somit die Patientenberichte pseudonymisiert weiterleiten können.

Da die Aufgaben der Personalabteilung lediglich die Personaladministration betreffen, können deren Angestellte auch nicht als Hilfspersonen der Ärzte qualifiziert werden. Der Datenbekanntgabe durch die Personalabteilung stand somit auch nicht das Berufsgeheimnis gemäss Art. 321 StGB entgegen.

Titel: Personendaten: Voraussetzung für Erhebung
URL: http://www.datenschutz.ch/themen/1303.php
Datum: 17.07.2007

05.

Personendaten: Voraussetzung für Erhebung

Werden Personendaten mit einem Fragebogen oder sonst systematisch erhoben, müssen Rechtsgrundlage und Zweck der Bearbeitung bekannt gegeben werden. Auch für die Datenbearbeitungen, deren Ergebnisse nicht publiziert werden, ist eine gesetzliche Grundlage notwendig.

Eine öffentlich-rechtliche Anstalt plante, dass die Studierenden die Lehrveranstaltungen beurteilen sollen. Die Ergebnisse dieser Evaluation sollten anschliessend veröffentlicht werden. Dabei stellte sich die Frage, ob es bei entsprechender gesetzlicher Grundlage möglich sei, die Resultate von allen Veranstaltungen sämtlichen Studierenden zur Kenntnis zu bringen oder ob dies in Bezug auf die Interessen der betroffenen Dozierenden unverhältnismässig wäre. Bei der Beurteilung beschränkte sich der Datenschutzbeauftragte auf die Frage der Veröffentlichung der Evaluationsergebnisse, zur Evaluation selbst äusserte er sich nicht.

Gemäss § 7 DSG sind Personendaten in der Regel bei der betroffenen Person zu beschaffen. Werden Personendaten systematisch, namentlich mit Fragebogen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung bekannt gegeben werden.

Für die Datenbekanntgabe durch öffentliche Organe ist § 8 Abs. 1 DSG massgebend. Personendaten dürfen bekannt gegeben werden, wenn eine gesetzliche Grundlage es erlaubt, wenn es im Einzelfall zur Erfüllung einer öffentlichen Aufgabe der Empfänger notwendig ist, wenn die betroffene Person im Einzelfall eingewilligt hat oder wenn sie ihre Daten allgemein zugänglich gemacht hat. Eine allfällige gesetzliche Grundlage müsste zudem dem Prinzip der Verhältnismässigkeit entsprechen (§ 4 Abs. 3 DSG).

Fraglich war, ob die Veröffentlichung der Evaluationsergebnisse für die Aufgabenerfüllung der öffentlich-rechtlichen Anstalt überhaupt geeignet und erforderlich ist. Da zudem nicht ersichtlich war, aus welchem Grund und mit welchem Zweck die Evaluationsergebnisse veröffentlicht werden sollten, empfahl der Datenschutzbeauftragte, vorläufig von einer Veröffentlichung abzusehen. Somit muss eine betroffene Person – also der oder die Dozierende – bis auf weiteres einwilligen, damit die Evaluationsergebnisse in Bezug auf ihre Veranstaltung veröffentlicht werden können.

Die öffentlich-rechtliche Anstalt hat darauf von einer Veröffentlichung der individuellen Umfrageergebnisse ohne ausdrückliche Einwilligung der betroffenen Person abgesehen. Vorgesehen ist allerdings die Veröffentlichung von aggregierten Daten, die keinen Rückschluss auf bestimmte oder bestimmbare Personen erlaubt.

Zu beachten ist, dass auch für Datenbearbeitungen, deren Ergebnisse nicht publiziert werden sollen, eine gesetzliche Grundlage geschaffen werden muss.

Titel: Denkmalschutzobjekte: Einsicht ins Inventar
URL: http://www.datenschutz.ch/themen/1304.php
Datum: 17.07.2007

06.

Denkmalschutzobjekte: Einsicht ins Inventar

Das Einsichtsrecht Dritter in die Natur- und Heimatschutzinventare gemäss Planungs- und Baugesetz (PBG) beschränkt sich auf die Daten, die zur Erfüllung des Inventarzwecks unbedingt nötig sind.

Eine Gemeinde setzte im Sinne von § 203 Abs. 2 PBG das überarbeitete Inventar über Denkmalschutzobjekte fest. Dazu wurde zu jeder Liegenschaft ein Inventar erstellt, welches in manchen Fällen auch Fotos aus dem Inneren des Gebäudes enthielt. Die Gemeinde gelangte nun mit der Anfrage an den Datenschutzbeauftragten, ob und in welchem Umfang Dritten ein Anspruch auf Einsicht und Kopien in das Inventar über denkmalgeschützte Objekte gewährt werden soll.

Sobald raumbezogene Daten einen Detaillierungsgrad aufweisen, der Gebäude und Adressen identifizierbar macht, handelt es sich um Personendaten. Und zwar in dem Sinne, dass mittels öffentlicher Register wie Grundbuch oder Telefonbuch ein Rückschluss auf Eigentümer, Bewohner und andere Berechtigte möglich ist. Inventarblätter enthalten somit selbst ohne Namensnennung der aktuellen und vergangenen Eigentümer Personendaten.

Wird Privatpersonen Einsicht in das Inventar gewährt, stellt dies eine Bekanntgabe von Personendaten im Sinne von § 8 DSG dar. Öffentliche Organe dürfen Personendaten bekannt geben, wenn dafür gesetzliche Grundlagen bestehen oder wenn

a) die Daten für den Empfänger im Einzelfall zur Erfüllung seiner öffentlichen Aufgabe notwendig sind;
b) die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf oder
c) die betroffene Person ihre Daten allgemein zugänglich gemacht hat.

Gemäss § 203 Abs. 2 PBG stehen die Natur- und Heimatschutzinventare bei der Gemeinde zur Einsicht offen. Allerdings dürfen nur Daten bearbeitet und zugänglich gemacht werden, die für die Erfüllung der öffentlichen Aufgabe geeignet und erforderlich sind (§ 4 Abs. 3 DSG; Erfordernis der Verhältnismässigkeit). Gemäss § 6 Abs. 1 der Natur- und Heimatschutzverordnung ist im Inventar eine knappe Umschreibung und Wertung des Objektes vorzunehmen, und die bestehenden Schutzmassnahmen sowie der Schutzzweck sind aufzuführen.

Für die erforderliche Verhältnismässigkeit empfiehlt der Datenschutzbeauftragte, im Exemplar, das zur Einsicht offensteht, zumindest allfällige Innenaufnahmen abzudecken. Falls der Zweck der öffentlichen Einsichtsmöglichkeit nach § 203 Abs. 2 PBG gewahrt werden kann, wäre es auch möglich, nur die erste Seite mit den Grunddaten des Inventars zur Einsicht freizugeben. In diesem Rahmen dürfen auch Kopien herausgegeben werden.

Titel: Anwendbares Datenschutzrecht für Stiftung
URL: http://www.datenschutz.ch/themen/1305.php
Datum: 17.07.2007

07.

Anwendbares Datenschutzrecht für Stiftung

In Bezug auf eine beitragsberechtigte privatrechtliche Stiftung muss in jedem Einzelfall separat abgeklärt werden, ob sie dem kantonalen oder dem eidgenössischen Datenschutzrecht untersteht.

Für eine privatrechtliche Stiftung stellte sich im Zusammenhang mit einem neuen Qualitätsmanagement die Frage, ob sie zürcherischem oder eidgenössischem Datenschutzrecht unterstellt ist. Unklar war auch die Anwendbarkeit des Amtsgeheimnisses. Die Stiftung finanziert sich hauptsächlich über die öffentliche Sozialhilfe und die IV-Stelle, erhält aber auch Subventionen sowie Defizitbeiträge vom Kanton Zürich. Zweck der Stiftung ist die Einrichtung und der Betrieb von therapeutischen Wohngemeinschaften für Personen mit Suchtproblemen. Die Personen treten entweder aufgrund einer Eingliederungsmassnahme gemäss Art. 8 IVG in die Wohngemeinschaft ein oder werden der Stiftung durch die Sozialhilfe- oder die Justizvollzugsbehörde zugewiesen.

Die Frage, ob das zürcherische oder das eidgenössische Datenschutzgesetz anwendbar ist, muss für jede Person separat beurteilt werden:

Aufenthalt als Eingliederungsmassnahme

Gemäss Art. 8 IVG haben Invalide oder von einer Invalidität unmittelbar bedrohte Personen Anspruch auf Eingliederungsmassnahmen. Die IV-Stelle ist für die Bestimmung und Überwachung der Eingliederungsmassnahmen zuständig (Art. 57 Abs. 1 lit. c IVG). Die kantonale IV-Stelle entscheidet, ob ein Gesuchsteller Anspruch auf Eingliederungsmassnahmen hat, und kontrolliert deren Durchführung. Die Massnahmen selber durchzuführen, gehört indes nicht zu ihren öffentlichen Aufgaben. Insofern erfüllt auch die mit der Durchführung betraute Stiftung keine öffentlichen Aufgaben und untersteht diesbezüglich dem eidgenössischen Datenschutzgesetz.

Zuweisung durch Behörden

Gemäss § 7 SHG ist die Fürsorgebehörde für die Gewährleistung der persönlichen Hilfe zuständig. Die Beratungs- und Betreuungsstellen bestimmen Art und Umfang der Hilfe. Soweit diese die Beratung und Betreuung nicht selber vornehmen oder wo spezialisierte Hilfe notwendig ist, vermitteln sie die Dienstleistungen anderer Stellen (§ 12 Abs. 2 und 3 SHG). Persönliche Hilfe kann unter anderem durch öffentliche oder private soziale Institutionen gewährt werden, denen die Gemeinde entsprechende Aufgaben ganz oder teilweise übertragen hat (§ 13 SHG).

Im Rahmen des Justizvollzugs werden Süchtige, die straffällig geworden sind und deren Straftat mit ihrer Abhängigkeit in Zusammenhang steht, behandelt (Art. 44 aStGB / Art. 60 nStGB). Die Behandlung kann gemäss Art. 384 aStGB (Art. 379 nStGB) sowie § 15 Justizvollzugsverordnung Einrichtungen mit privater Trägerschaft übertragen werden.

Die Gewährung persönlicher Hilfe und der Vollzug einer strafrechtlichen Massnahme sind demnach kantonale respektive kommunale Aufgaben, welche in bestimmten Fällen durch die private Stiftung erbracht werden. Diesbezüglich fällt die Stiftung unter das zürcherische Datenschutzgesetz.

Es stellt sich ausserdem die Frage, ob es sich bei der Stiftung, indem sie öffentliche Aufgaben übernimmt, um ein öffentliches Organ im Sinne von § 2 DSG handelt oder ob eine Auftragsdatenbearbeitung gemäss § 13 DSG vorliegt.

Indizien dafür, dass eine private Organisation in Bezug auf ihre Aufgabenerfüllung als öffentliches Organ zu betrachten ist, sind unter anderem: die Kompetenz, Verfügungen zu erlassen, die Einschränkung der Vertragsfreiheit, ein gesetzlicher Auftrag sowie die Subventionierung durch den Kanton. Zwischen den verschiedenen Elementen ist eine Gesamtabwägung zu treffen.

Im zu beurteilenden Fall untersteht die Stiftung der öffentlichen Aufsicht. Zudem erhält sie staatliche Subventionen sowie Defizitbeiträge. Zwar ist der gesetzliche Auftrag zur Durchführung von Sozialhilfemassnahmen und strafrechtlichen Massnahmen an die zuständigen staatlichen Stellen gerichtet, diese werden jedoch per Gesetz explizit dazu ermächtigt, die Durchführung Privaten zu übertragen. Im Falle von strafrechtlichen Massnahmen können die betroffenen Personen sogar gezwungen werden, sich bei der Stiftung behandeln zu lassen. In diesem Sinne ist auch die Vertragsfreiheit eingeschränkt. Bei der Datenbearbeitung im Rahmen der Sozialhilfemassnahmen und des Auftrages, den sie für das Amt für Justizvollzug durchführt, ist die Stiftung somit als öffentliches Organ im Sinne des § 2 DSG ZH zu betrachten.

Die Frage, welchem Recht die Stiftung untersteht, hat nur indirekt mit der Frage zu tun, ob deren Mitarbeitende dem Amtsgeheimnis unterstellt sind. Sie unterstehen jeweils dann dem Amtsgeheimnis, wenn auf die Stiftung entweder Art. 33 ATSG anwendbar ist oder diese eine öffentliche Aufgabe erfüllt.

Titel: Fördermassnahmen: Datenerhebung erleichtert
URL: http://www.datenschutz.ch/themen/1306.php
Datum: 17.07.2007

08.

Fördermassnahmen: Datenerhebung erleichtert

Bei Personendaten, die für nicht personenbezogene Zwecke – insbesondere in der Forschung, Planung und Statistik – bearbeitet werden, lässt das Datenschutzgesetz eine erleichterte Bearbeitung zu.

Zwecks Erhebung der sonderpädagogischen und unterrichtsergänzenden Angebote verlangte die Bildungsdirektion von den Schulgemeinden Listen mit Name und Geburtsdatum von allen Schülerinnen und Schülern, die sonderpädagogische Massnahmen benötigen. Ebenso sollte die Art der Fördermassnahme aufgeführt werden.

Namen und Geburtsdaten sind Personendaten im Sinne des DSG. Angaben über die geistige und körperliche Gesundheit (z.B. über die Notwendigkeit einer Psychotherapie) sind besonders schützenswerte Personendaten gemäss § 2 lit. d Ziff. 2 DSG. Gemäss § 5 DSG dürfen sie nur bearbeitet werden, wenn sich die Zulässigkeit aus einer gesetzlichen Grundlage klar ergibt, es zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich ist, die betroffene Person im Einzelfall eingewilligt, ihre Daten allgemein zugänglich gemacht hat oder ihre Zustimmung vorausgesetzt werden darf.

Werden Personendaten für nicht personenbezogene Zwecke bearbeitet, beispielsweise in der Forschung, Planung und Statistik, lässt § 12 DSG eine erleichterte Bearbeitung zu, da diese nach der Auswertung schnellstmöglich zu anonymisieren sind und die Ergebnisse nur so veröffentlicht werden dürfen, dass die betroffenen Personen nicht bestimmbar sind.

Gestützt auf § 3 der Verordnung über Datenbearbeitung im Bildungsbereich (Bildungsdatenverordnung) kann bei der Weitergabe von bestimmten, in Anhang 1 und 2 zur Bildungsdatenverordnung aufgeführten Daten auf eine Einzelfallprüfung im Sinne des Datenschutzgesetzes verzichtet werden. Anhang 1 nennt unter anderem Name, Vorname und Geburtsdatum sowie Auskünfte darüber, ob die Schulpflichtigen Stütz- und Fördermassnahmen benötigen. Die Bildungsdatenverordnung stellt die gesetzliche Grundlage dar, aufgrund deren die genannten Informationen nicht nur einzeln, sondern auch in Kombination miteinander an die Bildungsdirektion weitergegeben werden dürfen.

Der aus administrativen Gründen notwendige Personenbezug von Daten ist jedoch bei den Lernenden spätestens 10 Jahre nach der letzten Datenerfassung oder -mutation aufzuheben (§ 4 Abs. 4 Bildungsdatenverordnung). Zudem dürfen die Daten nur für planerische und statistische Zwecke verwendet werden; eine Verwendung für andere Zwecke ist unzulässig.

Die fraglichen Daten durften somit der Bildungsdirektion im Rahmen des vorgestellten Projekts bekannt gegeben werden.

Titel: Online-Angebot mit Einwilligung
URL: http://www.datenschutz.ch/themen/1307.php
Datum: 17.07.2007

09.

Online-Angebot mit Einwilligung

Die Gebäudeversicherung (GVZ) darf Banken, die im Hypothekargeschäft tätig sind, nur für jene Daten einen Online-Zugriff einrichten, für welche die Einwilligung der Gebäudeeigentümer vorliegt.

Die GVZ bat den Datenschutzbeauftragten, die Rechtmässigkeit eines Online-Zugriffes auf Gebäudedaten für Banken, die im Hypothekargeschäft tätig sind, zu prüfen (siehe Tätigkeitsbericht Nr. 11 [2005], S. 74 f.). Nun legte sie ihm das Grobkonzept «Zugriff auf GVZ-Daten für Hypothekargeschäfte» zur Prüfung und Stellungnahme vor.

Das Grobkonzept sieht vor, dass ausgewählte Banken Zugriff auf die Daten jener Gebäudeeigentümer erhalten, die ihre Einwilligung zur Datenbekanntgabe erteilt haben. Die elektronische Plattform dazu soll die Abteilung für Datenlogistik (DLG) der Baudirektion betreiben. Die DLG ist bereits Betreiberin des DLG-Auskunftssystems (AKS) für die Gebäudedaten innerhalb des Kantons. Das bestehende AKS soll nun für die elektronische Datenabgabe an Banken genutzt werden. Die GVZ und die DLG müssen sicherstellen, dass die Daten nur im Rahmen der gesetzlichen Bestimmungen genutzt werden können.

Die wesentliche Änderung des neuen Konzepts besteht darin, dass die Banken nur Zugriff auf jene GVZ-Daten erhalten, für welche die Gebäudeeigentümer ihre Einwilligung erteilt haben. Eine Zugriffsberechtigung auf alle Gebäudedaten wird nicht eingerichtet. Zu beachten sind die weiteren Voraussetzungen wie Verhältnismässigkeit, Zweckbindung sowie keine Weitergabe an Dritte (siehe Tätigkeitsbericht Nr. 4 [1998], S. 41 f.).

Der Entscheid über die Authentifizierungsform der Einwilligung obliegt der GVZ.

Aufgrund der Unterlagen ging der Datenschutzbeauftragte davon aus, dass die GVZ-Daten in keiner Form anderen Stellen zur Verfügung gestellt werden. Andernfalls wäre eine genügende gesetzliche Grundlage erforderlich. Die Datensicherheitsmassnahmen richten sich nach den Anforderungen der Informatiksicherheitsverordnung. Die applikationsspezifischen Risiken sind aufzuzeigen, und entsprechende Massnahmen sind einzuleiten.

Titel: Daten an die Sozialversicherung
URL: http://www.datenschutz.ch/themen/1308.php
Datum: 17.07.2007

10. Daten an die Sozialversicherung

Personendaten sind in der Regel bei der betroffenen Person zu beschaffen. Verfügt die betroffene Person nicht über die verlangten Angaben, hat sie in einem zweiten Schritt dem bearbeitenden Organ eine Ermächtigung zur Datenbekanntgabe zu erteilen.

Ein Lehrer, dessen Arbeitsverhältnis durch eine Vereinbarung mit der Schulpflege beendet worden war, erhob beim zuständigen Sozialversicherungsorgan Einsprache gegen die Verfügung der Arbeitslosenkasse betreffend Auferlegung von Einstelltagen. In diesem Zusammenhang stellten sich seitens des Sozialversicherungsorgans diverse Fragen zur Beendigung des Arbeitsverhältnisses. Es verlangte deshalb von der Schulpflege Akteneinsicht in das Personaldossier des Lehrers sowie die Herausgabe der Gesprächsprotokolle. In der Folge gelangte die Schulpflege mit der Anfrage an den Datenschutzbeauftragten, ob und in welchem Masse sie zur Auskunft und Akteneinsicht gegenüber dem Sozialversicherungsorgan verpflichtet sei.

Für die Datenbekanntgabe durch öffentliche Organe ist § 8 Abs. 1 DSG massgebend. Gemäss dieser Norm dürfen Personendaten nur in folgenden Fällen bekannt gegeben werden: wenn eine gesetzliche Grundlage es erlaubt, wenn es im Einzelfall zur Erfüllung einer öffentlichen Aufgabe der Empfänger notwendig ist oder wenn die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht hat.

In der Regel sind Personendaten bei der betroffenen Person zu beschaffen (§ 7 Abs. 1 DSG). Für die vom Sozialversicherungsorgan verlangten Personendaten ergibt sich das zudem aus Art. 28 ATSG (Mitwirkung beim Vollzug). Verfügt die betroffene Person nicht über die verlangten Angaben, hat sie in einem zweiten Schritt der Schulpflege eine entsprechende Ermächtigung gemäss Art. 28 Abs. 3 ATSG – welche einer Einwilligung gemäss § 8 Abs. 1 lit. b DSG entspricht – zu erteilen. Die Schulpflege als Arbeitgeberin gibt – gestützt auf diese Ermächtigung – anschliessend die entsprechende Auskunft an das Sozialversicherungsorgan.

Titel: Auskünfte der Einwohnerkontrolle
URL: http://www.datenschutz.ch/themen/1309.php
Datum: 17.07.2007

11. Auskünfte der Einwohnerkontrolle

Private Personen und Organisationen können der Einwohnerkontrolle Gesuche für die Bekanntgabe von Personendaten stellen. Die Voraussetzungen für die Bekanntgabe sind unterschiedlich.

Die Einwohnerkontrolle gibt gemäss Datenschutzgesetz einer privaten Person oder Organisation im Einzelfall auf Gesuch hin bestimmte Daten bekannt (§ 9 DSG). Je nachdem, welche Daten gewünscht werden oder ob eine Datensperre besteht, gelten für die Bekanntgabe verschiedene Voraussetzungen.

Die Einwohnerkontrolle muss in jedem Fall zuerst prüfen, ob durch die Bekanntgabe wesentliche öffentliche Interessen oder offensichtlich schützenswerte Interessen einer betroffenen Person verletzt werden (§ 10 DSG). Die Praxis zeigt jedoch, dass Routineauskünfte gemäss § 9 Abs. 1 und 2 DSG nur selten eingeschränkt werden müssen.

Wer sich ausgewiesen hat, kann von der Einwohnerkontrolle Auskunft darüber verlangen, welche Daten zur eigenen Person in den Datensammlungen der Einwohnerkontrolle bearbeitet werden (§ 17 DSG). Das Auskunftsrecht gilt sowohl für die Person, die von der Einwohnerkontrolle Daten verlangt hat, als auch für jene Person, über welche Einwohnerkontrolldaten verlangt wurden. Letztere muss auf Verlangen darüber informiert werden, wer welche Daten über sie erhalten hat.

Das gegenseitige Auskunftsrecht ist bei der Organisation der Akten-/Datenablage zu berücksichtigen. Daten dürfen jedoch nur bearbeitet werden, soweit dies für die Erfüllung der Aufgaben geeignet und erforderlich ist (§ 4 Abs. 3 DSG). Schriftliche Unterlagen zu Routineauskünften gemäss § 9 Abs. 1 und 2 DSG können in der Regel nach Erledigung vernichtet werden. Mündliche Auskünfte hingegen müssen nicht dokumentiert werden. Sind Dokumente nach Ablauf der Aufbewahrungsfrist vernichtet worden, entfällt das Auskunftsrecht ganz. Einzelne Einschränkungen der Bekanntgabe sind gemäss § 10 DSG und § 18 DSG möglich.

Einer Person, die in einer Liste, beispielsweise einer Adressliste, verzeichnet ist, steht das Auskunftsrecht gemäss § 9 Abs. 3 DSG zu, sofern die bekannt gegebenen Daten nach ihr erschliessbar sind.

Die Einwohnerkontrolle muss für die verschiedenen Arten der Datenbekanntgabe gemäss § 9 DSG festlegen, welche Dokumente für wie lange aufbewahrt werden müssen (§ 14 Abs. 2 DSG). Diese Regeln gelten nur für die Dokumente zur Datenbekanntgabe an Personen. Buchhaltungsunterlagen, die für einen anderen Zweck erstellt und aufbewahrt werden müssen, müssen getrennt verwaltet werden.

Titel: Keine Steuerdaten für Stadtmarketing
URL: http://www.datenschutz.ch/themen/1310.php
Datum: 17.07.2007

12.

Keine Steuerdaten für Stadtmarketing

Will das Steueramt Angaben, welche ihm zur Steuereinschätzung bekannt gegeben werden, zu einem anderen Zweck verwenden, braucht es eine entsprechende gesetzliche Grundlage oder eine vorgängige Einwilligung der betroffenen Person.

Zum Zwecke des Stadtmarketings beabsichtigte eine Gemeinde, Liegenschaften, die über einen hohen Anteil an unbebauter Wohnfläche verfügen, zu evaluieren. Das Steueramt bereitete dazu die relevanten Personendaten ausgewählter Steuerpflichtiger auf. Im Auftrag des Stadtmarketings fragte das Steueramt diese Steuerpflichtigen schriftlich an, ob sie bereit seien, einige Fragen zu ihrer Liegenschaft zu beantworten. Die Teilnahme wurde ausdrücklich als freiwillig bezeichnet.

Die dazu verwendeten Angaben erhielt das Steueramt zuvor von Notariaten und Grundbuchämtern. Diese sind gegenüber dem Steueramt verpflichtet, an der Vorbereitung und Durchführung von Steuereinschätzungen mitzuwirken und aus ihren Akten Auskunft zu erteilen (§ 209 Abs. 2 Steuergesetz sowie §§ 67 ff. Verordnung zum Steuergesetz).

Aufgrund zweier separat eingereichter Aufsichtsbeschwerden gelangte der Bezirksrat an den Datenschutzbeauftragten und bat um die Beurteilung der Frage, ob die Bearbeitung folgender Personendaten rechtmässig erfolgt war: Namen der Eigentümerinnen oder Eigentümer, Name der Verwalterin oder des Verwalters, Katasternummer, Parzellenadresse, Parzellenfläche und Anteil an unbebauter Wohnfläche.

Gemäss § 4 Abs. 4 DSG dürfen Daten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird. Dieses Zweckbindungsgebot erlaubt aus Gründen der Transparenz sowie der Rechtssicherheit nur dann eine Zweckänderung, wenn eine entsprechende Rechtsgrundlage oder die vorgängige Einwilligung der betroffenen Person vorliegt.

Die Bekanntgabe der Daten durch die Notariate und Grundbuchämter an das Steueramt erfolgte ursprünglich zum Zweck der Steuereinschätzung. Die nachfolgende Datenaufbereitung und -verwendung durch das Steueramt erfolgte nicht zur eigenen Aufgabenerfüllung gemäss den rechtlichen Grundlagen im Steuerrecht, sondern zu einem weiteren, ausserhalb des Aufgabenbereiches des Steueramtes liegenden Zweck. Dabei wurde weder die Rechtsgrundlage angepasst, noch lag die Einwilligung der betroffenen Personen vor. Die freiwillige Beantwortung der späteren Umfrage bei den Steuerpflichtigen ändert an der unerlaubten Zweckänderung nichts, da die Datenbearbeitung stattgefunden hatte, bevor die betroffenen Personen ihr Einverständnis dazu geben konnten.

Titel: Schützenswerte Interessen prüfen
URL: http://www.datenschutz.ch/themen/1311.php
Datum: 17.07.2007

13.

Schützenswerte Interessen prüfen

Kommt ein öffentliches Organ vorerst zum Schluss, dass eine Datenbekanntgabe zu erfolgen hat, muss es zudem die Umstände des Einzelfalles berücksichtigen und prüfen, ob offensichtlich schützenswerte Interessen des Betroffenen eine Einschränkung verlangen.

Eltern wollten ihre Tochter, die den Kindergarten besuchte, frühzeitig einschulen lassen. Die zuständige Schulleitung beauftragte deshalb den Schulpsychologischen Beratungsdienst (SPD) mit diversen Abklärungen, inklusive Befragung der beiden Kindergärtnerinnen. Hinsichtlich dieser Befragung baten die Eltern den SPD ausdrücklich, wegen früherer Vorkommnisse lediglich eine der beiden Kindergärtnerinnen in die Abklärungen zu involvieren. Der SPD insistierte jedoch auf einen Einbezug der zweiten Kindergärtnerin und leitete dieser – ohne die Eltern darüber zu informieren – eine Kopie des schulpsychologischen Abklärungsberichts weiter.

Der SPD begründet dieses Vorgehen damit, dass es Aufgabe des beauftragten Schulpsychologen sei, zu entscheiden, welche sachdienlichen Informationen nötig seien. Dazu gehörten auch Auskünfte der Kindergärtnerinnen. Zudem entspreche eine Berichterstattung an die Kindergärtnerinnen den internen Richtlinien.

Personendaten, welche durch den SPD erhoben werden, sind im Sinne von § 2 lit. d Ziff. 2 DSG. besonders schützenswert. Sie dürfen von öffentlichen Organen nur bekannt gegeben werden, wenn dies aufgrund einer gesetzlichen Grundlage klar zulässig ist, wenn es zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich ist oder wenn im Einzelfall die Einwilligung der betroffenen Person vorliegt (§ 5 DSG).

Eine klare gesetzliche Grundlage für die Datenbekanntgabe war im konkreten Fall nicht bekannt. Von einer Einwilligung der betroffenen Person respektive deren Eltern war ebenfalls nicht auszugehen. Offen war jedoch, ob die Bekanntgabe des vollständigen Abklärungsberichts der Tochter für die Kindergärtnerin zur Erfüllung ihrer gesetzlichen Aufgaben unentbehrlich war.

Ginge es im besagten Bericht lediglich um die Frage der Schulreife, würde es genügen, wenn nur das Ergebnis mitgeteilt würde: So wüsste die Kindergärtnerin, ob das Kind weiterhin bei ihr verbleiben würde. Enthielte der Bericht jedoch Angaben, welche für die konkrete Arbeit der Lehrperson mit dem Kind notwendig wären, wäre die Bekanntgabe möglicherweise zu Recht erfolgt.

Obwohl die Bekanntgabe des Berichts an die Kindergärtnerin oder an die Lehrperson wohl in den meisten Fällen den Bedürfnissen aller Beteiligten sowie den Vorgaben gemäss den erwähnten Richtlinien entspricht, müssen immer auch die Umstände des Einzelfalls geprüft werden. Das Begehren der Eltern, der Kindergärtnerin den Bericht nicht zukommen zu lassen, ist im Einzelfall bei der Prüfung der Bekanntgabe zumindest zu berücksichtigen. Wird trotzdem eine Bekanntgabe beschlossen, ist dies zu begründen.

Ausschlaggebend war somit im vorliegenden Fall nicht in erster Linie, ob die Eltern eine Datenbekanntgabe untersagt hatten oder nicht, da die Schulgemeinde den Auftrag zur Abklärung

beim SPD erteilt hatte. Eine Einwilligung oder Untersagung der Eltern wäre jedoch im Rahmen der Güterabwägung von § 10 DSG zu berücksichtigen gewesen.

Eine bereits vorgängig explizit nicht erteilte Einwilligung der Eltern ist somit im konkreten Einzelfall im Rahmen der Güterabwägung zu prüfen. Kommt das öffentliche Organ in einem ersten Schritt zum Schluss, dass eine Datenbekanntgabe zu erfolgen hat, hat es in einem weiteren Schritt zu prüfen, ob offensichtlich schützenswerte Interessen des betroffenen Kindes eine Einschränkung gemäss § 10 DSG verlangen.

Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

Datenschutzbeauftragter
Dr. iur. Bruno Baeriswyl

Stellvertreter
lic. iur. Beda Harb

Juristisches Sekretariat
lic. iur. Barbara Mathis
lic. iur. Karin Schoch
lic. iur. Karin Brunner Steib
Dr. iur. Claudia Mund

IT-Revision und -Kontrolle
Andrea C. Mazzocco, CISA

Beratungsstelle für Informatiksicherheit (BIS)
vakant

Kommunikation
Dr. phil. Andrea Ruf

Sekretariat
Martina Richard

Tätigkeitsbericht Nr. 12 (2006)
ISSN 1422-5816

Gestaltung
Fabian Elsener Mediengestaltung, Zürich

Druck
KDMZ
Gedruckt auf Recyclingpapier

Bezug
Datenschutzbeauftragter des Kantons Zürich
Postfach, 8090 Zürich
Tel.: 043 259 39 99
Fax: 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

www.datenschutz.ch