Nummer 13

Tätigkeitsbericht 2007

Datenschutz
mit Qualität

datenschutzbeauftragter
kanton zürich

Nummer 13
Tätigkeitsbericht 2007

Der Datenschutzbeauftragte erstattet dem Regierungsrat jährlich oder nach Bedarf einen Bericht über seine Tätigkeit (§ 23 Datenschutzgesetz). Der vorliegende Tätigkeitsbericht Nr. 13 [2007] deckt den Zeitraum vom 1. Januar 2007 bis 31. Dezember 2007 ab.

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

Zürich, Juni 2008

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. VERNEHMLASSUNGEN

V. SICHERHEIT UND KONTROLLE

VI. INFORMATION

VII. ANHANG

Verantwortung der öffentlichen Organe nimmt zu

Die öffentlichen Organe sind immer stärker gefordert, das Grundrecht auf Datenschutz zu gewährleisten. Die Risiken für die Bürgerinnen und Bürger nehmen zu.

Die Herausforderungen im Bereich des Datenschutzes für die öffentlichen Organe im Kanton Zürich haben auch im vergangenen Jahr nicht abgenommen. Immer mehr zeigt sich die filigrane Verknüpfung auch der noch so kleinen Verwaltungseinheit mit der globalen Informations- und Kommunikationsgesellschaft. Dabei werden sehr schnell die globalen Risiken auch im lokalen Bereich ersichtlich:

Als eine Zürcher Gemeinde eine Liste ihrer Feuerwehr-Kadermitglieder mit den Kontaktadressen auf ihrer Homepage veröffentlichte, dachte sie in erster Linie daran, der Bevölkerung die Ansprechmöglichkeiten zu erleichtern. In der Zwischenzeit hat einer der Feuerwehrleute eine Anstellung in einem Sicherheitsbereich angenommen. Aus diesem Grund und um mögliche Bedrohungen zu vermeiden, ist er darauf angewiesen, dass seine Wohnadresse nicht allgemein bekannt ist. Er bat deshalb die Gemeinde, seine Adresse von der Homepage zu entfernen, was diese umgehend veranlasste. Er staunte indessen nicht schlecht, als sein Name und seine Adresse weiterhin durch die Suchmaschinen im Internet auffindbar blieben. Denn Suchmaschinen indexieren laufend die Websites im Internet, um sie schneller verfügbar zu machen. Ist der Eintrag auf einer Website aber einmal geändert, werden die alten Seiten nicht zwangsläufig gelöscht. Vielmehr verbleiben sie noch Monate im Speicher der Suchmaschinen und können immer wieder gefunden werden. Und sie werden kopiert von anderen Websites und damit weiterverbreitet oder sie landen im Archiv des Internets, wo sämtliche Internetseiten periodisch abgelegt werden (www.archive.org). Mit anderen Worten: Das Internet vergisst nicht. Oder: Was einmal im Internet steht, bleibt ewig vorhanden. Die Konsequenzen für den betroffenen Feuerwehrmann: Er muss mit der möglichen Bedrohung leben oder er muss seinen Wohnort wechseln.

An der Bekanntgabe von Personendaten im Internet zeigen sich zwei Aspekte der Informations- und Kommunikationsgesellschaft deutlich: Erstens trägt jede Datenbearbeitung das Potenzial einer Persönlichkeitsverletzung und bedeutet daher einen Eingriff in die Grundrechte. Zweitens sind die Risiken für die Privatheit der betroffenen Personen zunehmend, insbesondere aufgrund der technologischen Möglichkeiten.

Grundrecht auf Datenschutz

Die Erkenntnis, dass eine Datenbearbeitung das Grundrecht auf persönliche Freiheit und Privatsphäre beeinträchtigen könnte, ist schon früh gereift – bereits beim Aufkommen der Grosscomputer und bei deren kommerzieller Verbreitung

in den 1960er Jahren. Die Möglichkeit, eine grosse Menge Daten über einzelne Bürgerinnen und Bürger zentral zu speichern, insbesondere durch den Staat, gab zu Besorgnis Anlass, dass die staatlichen Datenbearbeitungen überhandnehmen und die Freiheitsrechte ernsthaft bedrohen könnten. Ein Eingriff in die persönliche Freiheit und in das Grundrecht auf Privatheit ist indessen nur dann erlaubt, wenn eine ausreichende gesetzliche Grundlage die Datenbearbeitung rechtfertigt. Dieser Grundsatz findet sich heute sowohl in der Bundesverfassung (Art. 36 BV) als auch in der Kantonsverfassung (Art. 38 lit. b KV). Es galt deshalb, neben diesem Grundsatz die weiteren Rahmenbedingungen für die Datenbearbeitungen zu konkretisieren: Sie müssen auf ein Mass eingeschränkt werden können, welches die Grundfreiheiten der Bürgerinnen und Bürger respektiert.

In den Datenschutzgesetzen wurden die Rahmenbedingungen deshalb konkretisiert. Zu diesen Grundsätzen gehören das Prinzip der Verhältnismässigkeit, wonach eine Datenbearbeitung für die Aufgabenerfüllung geeignet und erforderlich sein muss, und das Prinzip der Zweckbindung, das besagt, dass die Verwendung der Daten nur für einen von vornherein festgelegten Zweck erfolgen kann. Aber auch die Richtigkeit und Vollständigkeit der Daten muss gewährleistet sein, und die Daten müssen gegen den Missbrauch geschützt sein. Mit diesen Prinzipien wird gegenüber den Bürgerinnen und Bürgern Transparenz geschaffen: Sie müssen sich darauf verlassen können, dass öffentliche Organe nur unter diesen Voraussetzungen Daten bearbeiten.

Vom DSG zum IDG

Relativ spät – lediglich im Mittelfeld der Kantone – hat der Kanton Zürich 1995 sein Datenschutzgesetz in Kraft gesetzt. Dieses wird nun von einem neuen Informations- und Datenschutzgesetz (IDG) abgelöst, das einige Neuerungen bringt, aber an den bewährten Prinzipien festhält. Die Neuerungen beziehen sich insbesondere auf die Schnittstelle zum neu eingeführten Öffentlichkeitsprinzip sowie auf Anpassungen an europarechtliche Vorgaben und an neuere Entwicklungen in der Technologie.

Technologische Entwicklung

Die heutigen technologischen Möglichkeiten der Informationsbearbeitung überschreiten bei weitem die Vorstellungen, wie sie noch 1995 bei der Einführung des DSG vorherrschten. Zwar waren die Dezentralisierung der Computer und deren Vernetzung schon weit fortgeschritten, doch die Dimensionen der globalen Vernetzung über das Internet nur in den Anfängen erkennbar. Die Speicherung von enormen Mengen von Daten ist heute weder eine technische noch eine finanzielle Frage: Sie ist eine Selbstverständlichkeit wie die Nutzung der Informations- und Kommunikationstechnologie im privaten und im geschäftlichen Umfeld.

Ebenso wachsen aber auch die Risiken für die Privatheit der Bürgerinnen und Bürger. Nicht nur die Menge der Daten ist zunehmend, auch die Tatsache, dass jede Nutzung von Informations- und Kommunikationstechnologien Spuren hinterlässt, ist zu bedenken: In der digitalen Welt erfolgt kein Schritt mehr unbeobachtet! Und diese Informationen bleiben «ewig» zur Verfügung. Es ist unschwer festzustellen, dass sich hier mosaikhaft der gläserne Bürger am Horizont abzeichnet, wenn nicht Gegenmassnahmen getroffen werden.

Die Verantwortung der Verwaltung

Diese Entwicklung entscheidet sich im Kleinen, wie die Publikation auf der Website der Gemeinde zeigt. Insbesondere bei Datenbekanntgaben kommt den öffentlichen Organen eine grosse Verantwortung zu. Vielfach verfügen sie über Informationen, die ihnen die Bürgerinnen und Bürger mitteilen müssen (zum Beispiel Angaben in der Steuererklärung), die nur sie kennen (zum Beispiel Angaben über strafrechtliche Verfahren) oder die besonders sensibel sind (zum Beispiel Angaben über die Gesundheit). Während es offensichtlich ist, dass solche Daten nur beschränkt an Dritte weitergegeben werden (zum Beispiel Angaben über das versteuerte Einkommen und Vermögen an Dritte ohne Interessennachweis), scheinen andere Informationen problemlos zu sein. Deshalb werden viele Informationen statistisch aufbereitet und im Internet zur Verfügung gestellt – beispielsweise die Bevölkerungsstruktur (Alter, Ausländeranteil) oder die Lageklasse einer Liegenschaft. Aber auch – wie gesehen – die Adresse des Kadermitgliedes der Feuerwehr. Ohne weiteres wird daraus ersichtlich, ob diese Person in einer teuren Wohngegend wohnt oder in einem Gebiet mit hohem Ausländeranteil. Der private Datenbearbeiter ist nicht weit, der diese Informationen aufbereitet und sie beispielsweise zu Marketingzwecken verarbeitet.

Bei der Datenbekanntgabe trägt das öffentliche Organ eine hohe Verantwortung. Nicht nur hat es abzuklären, ob Voraussetzungen für eine Datenbekanntgabe und mithin die Rahmenbedingungen der Datenschutzgesetzgebung gegeben sind (siehe oben), sondern auch, ob die Publikation beispielsweise im Internet nicht zu unnötigen Risiken für die betroffenen Personen führen kann.

Schlüsselrolle Gesetzgeber

Angesichts der geschilderten Risiken scheint es klar, dass bestehende Gesetzesgrundlagen, die eine Bekanntgabe von Daten an Dritte vorsehen, nur restriktiv ausgelegt werden können. Sieht ein Gesetz vor, dass Daten publiziert werden können, heisst dies nicht automatisch, dass dies auch eine Publikation im Internet bedeuten soll. Hier gilt es, die spezifischen Risiken zu berücksichtigen. Damit ist auch der Gesetzgeber gefordert. Immer mehr gilt es, klare Grundlagen für die wachsende Vernetzung der Informationsbestände der öffentlichen Organe zu schaffen. Dabei kommt den Regeln für die Datenbekanntgabe eine besondere Bedeutung zu. Nur wenn diese Datenbearbeitungen unter der vollen Respektierung der datenschutzrechtlichen Grundsätze erfolgen, können auch die Grundrechte der Bürgerinnen und Bürger gewährleistet werden.

Die Dynamik der technologischen Entwicklungen und das wachsende Bedürfnis nach immer mehr Informationen sind eine besondere Herausforderung für den Gesetzgeber. Es gilt, das technisch Mögliche zu hinterfragen und das Ziel der Datenbeschaffung kritisch zu beurteilen. Nur wenn das öffentliche Interesse an der Datenbearbeitung gegeben ist, das Ziel der Datenbearbeitung klar ist und die zu bearbeitenden Daten geeignet und erforderlich sind, ist der Eingriff in die persönliche Freiheit der Bürgerinnen und Bürger zu rechtfertigen.

Zunehmende Sensibilisierung

Nicht nur die öffentlichen Organe, sondern auch die Bürgerinnen und Bürger sind zunehmend sensibilisiert in Bezug auf den Umgang mit Personendaten. Allerdings sind die Unterschiede sehr gross. Während ein Grossteil der öffentlichen Organe umsichtig mit Personendaten umgehen, neue Projekte rechtzeitig

auf ihre Risiken in Bezug auf die Persönlichkeitsrechte der betroffenen Personen hin prüfen und angemessene Lösungen finden, sind andere sich der zunehmenden Herausforderungen im Bereich des Datenschutzes nicht bewusst. Ebenso ist bei den Bürgerinnen und Bürgern festzustellen, dass viele im eigenen Umfeld sorglos mit sensibelsten Informationen umgehen, hingegen manchmal bei geringfügigen Beeinträchtigungen ihrer Privatheit sehr stark reagieren können. In Zukunft wird es darum gehen, die unterschiedlichen Einstellungen der öffentlichen Organe und die unterschiedlichen Erwartungshaltungen der Bürgerinnen und Bürger in Bezug auf den Umgang mit Personendaten auszudiskutieren. Der Stellenwert des Datenschutzes in der Informations- und Kommunikationsgesellschaft hängt im Wesentlichen davon ab, mit welcher Konsequenz die öffentlichen Organe die datenschutzrechtlichen Rahmenbedingungen umsetzen und wie weit die Bürgerinnen und Bürger ihr Recht auf Privatheit einfordern. Letztendlich geht es aber wiederum um unsere liberale Rechts- und Gesellschaftsordnung und um die Umsetzung der Grundrechte in der Informations- und Kommunikationsgesellschaft. Der Datenschutz ist dabei ein Schlüsselelement.

Breites Themenspektrum

Der vorliegende 13. Tätigkeitsbericht für das Jahr 2007 zeigt ein breites Themenspektrum im Bereich des Datenschutzes auf. Datenbearbeitungen im Gesundheitswesen – insbesondere die Datenbekanntgabe von Spitälern an Versicherer – erweisen sich als besonders heikel, da von den Versicherern immer mehr sensible Gesundheitsdaten verlangt werden. Die Ärzte und Spitäler haben dabei das Patientengeheimnis zu respektieren (siehe Seite 10 f.). Der Aufbau von verschiedenen grossen Datenbeständen birgt das Risiko der Verknüpfung von unterschiedlichsten Daten zu Persönlichkeitsprofilen von Bürgerinnen und Bürgern. Eine transparente Gesetzgebung, welche die datenschutzrechtlichen Rahmenbedingungen respektiert, fehlt (siehe Seite 12 f.). Eine Auswahl von weiteren Themen zeigt, dass die Fragen im Zusammenhang mit dem Datenschutz vielfach komplex sind.

Aufgaben des Datenschutzbeauftragten

In diesem Umfeld unterstützt der Datenschutzbeauftragte die öffentlichen Organe mit Beratungen und Stellungnahmen. Eine wachsende Bedeutung kommt aber der regelmässigen Kontrolle der Datenbearbeitungen zu. Dabei lassen sich nicht nur Lücken feststellen, sondern mittels gezielter Hinweise oftmals auch klare Verbesserungen der Datenbearbeitungen in puncto Sicherheit erreichen. Auch Aus- und Weiterbildungsmassnahmen unterstützen die Verwaltung bei der Wahrnehmung ihrer Aufgaben im Bereich des Datenschutzes.

Bürgerinnen und Bürger wenden sich an den Datenschutzbeauftragten, um Auskunft über ihre Rechte zu erhalten oder weil sie konkrete Fragen zu sie betreffenden Datenbearbeitungen haben. Anfragen von betroffenen Personen führen dabei auch immer wieder zu Rückfragen bei den verantwortlichen öffentlichen Organen oder geben Anlass zu gezielten Kontrollen.

Auch in diesem Berichtsjahr hat sich gezeigt, dass die Dynamik der Informations- und Kommunikationsgesellschaft die Verwaltung voll erfasst hat und damit die Fragen des Datenschutzes bei allen Datenbearbeitungen immer präsenter wurden. Diese Entwicklung wird wohl mit neuen Technologien noch weiter zunehmen.

Handlungsbedarf für Patientengeheimnis

Die regelmässige Herausgabe der vollständigen Austritts- und Operationsberichte durch die Spitäler an die Unfall- und Krankenversicherer zur Überprüfung einzelner Rechnungen verletzt das Patientengeheimnis. Versicherer und eidgenössische Aufsichtsbehörden schenken dem Schutz des Patientengeheimnisses nicht die notwendige Beachtung.

Immer häufiger verlangen die Versicherer von den Spitälern ohne Begründung die Herausgabe der gesamten Austritts- oder Operationsberichte. Sie berufen sich darauf, dass sie ihre Leistungspflicht abklären und auch entscheiden müssten, wie viel und wie lange sie für einen Versicherten zahlen müssten.

Die Spitäler, die durch die verlangte Datenbekanntgabe das Patientengeheimnis gefährdet sehen, wenden sich immer häufiger an den Datenschutzbeauftragten.

Besonders schützenswerte Personendaten

Mit dem Austrittsbericht informieren die Spitäler den nachbehandelnden Arzt über den Spital- oder Heimaufenthalt eines Patienten. Der Austrittsbericht enthält sämtliche Diagnosen, aber auch Kommentare und Empfehlungen, wie der Arzt den Patienten nach der Spitalentlassung behandeln soll. Der Operationsbericht beschreibt den Operationsverlauf mit sämtlichen medizinischen Details.

Austritts- und Operationsberichte enthalten somit besonders schützenswerte Personendaten. Wenn Austritts- oder Operationsberichte an Dritte weitergegeben werden, handelt es sich um eine Datenbearbeitung besonderer Personendaten, an welche erhöhte rechtliche Anforderungen gestellt werden: Für eine solche Datenweitergabe braucht es eine gesetzliche Grundlage.

Die rechtliche Grundlage für die Beschaffung von Patientendaten bietet je nach Ereignis das Krankenversicherungsgesetz (KVG) oder das Unfallversicherungsgesetz (UVG).

Konstellationen für Datenweitergabe …

Die Krankenversicherer dürfen gemäss KVG in zwei Konstellationen Auskünfte der Spitäler und anderer Leistungserbringer erfragen. Eine Konstellation ist die Rechnungskontrolle: Die Krankenversicherung überprüft einzelne Rechnungen, bei welchen sie die Vergütung übernimmt und dem Versicherten somit die Kosten zurückerstattet (Art. 42 KVG). Die andere Konstellation ist die Wirtschaftlichkeitskontrolle (Art. 56 KVG).

Zum regelmässigen Datenfluss zwischen Leistungserbringern und Versicherern gehören detaillierte und verständliche Rechnungen sowie sämtliche Angaben, die der Versicherer benötigt, um die Vergütung berechnen und die Wirtschaftlichkeit der Leistung überprüfen zu können.

Der Versicherer kann im Einzelfall eine genaue Diagnose sowie zusätzliche medizinische Auskünfte verlangen. Dabei gilt, dass der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet ist, medizinische Angaben nur dem Vertrauensarzt oder der Vertrauensärztin des Versicherers bekannt zu geben (Art. 42 Abs. 3 und 4 KVG).

Beide Konstellationen bedingen keineswegs, dass die regelmässige Datenweitergabe immer auch eine detaillierte Diagnose enthalten muss. Vielmehr bezieht sich das Recht der Versicherer, eine detaillierte Diagnose zu erhalten, auf den Einzelfall und kann nur auf Anfrage gewährt werden.

Für die Unfallversicherer gelten zwar andere Rechtsgrundlagen als für Krankenversicherer; Wortlaut und Bedeutung stimmen jedoch mit den Regelungen im KVG überein. Anders als Krankenversicherer können Unfallversicherer breitere Abklärungen vornehmen (Untersuchungsgrundsatz). Die Unfallversicherer erhalten aber nicht uneingeschränkten Zugang zu den Patientendaten, da auch hier nur geeignete und erforderliche Daten weiterzugeben sind.

… müssen verhältnismässig sein

Ob eine Datenweitergabe verhältnismässig ist oder nicht, wird anhand der Kriterien Eignung und Erforderlichkeit beurteilt. Geeignet ist die Datenweitergabe dann, wenn sie den verfolgten Zweck erfüllt – wenn somit der Versicherer mit den erhaltenen Daten seine Aufgabe erfüllen kann. Die Erforderlichkeit entscheidet, ob und in welchem Ausmass eine Datenweitergabe notwendig ist – welche Daten also für die Aufgabenerfüllung absolut

unabdingbar sind (so genanntes mildestes Mittel). Bei beiden Kriterien ist somit der verfolgte Zweck der Datenerhebung wesentlich – der jedoch variieren kann: Ein Versicherer benötigt für die Rechnungskontrolle eine andere Datenmenge als für die Wirtschaftlichkeitskontrolle.

Im Rahmen der Rechnungskontrolle muss der Versicherer die Rechnungsstellung der Leistungserbringer überprüfen. Zu diesem Zweck verlangt das Gesetz von den Leistungserbringern eine detaillierte und verständliche Rechnung, die für die Überprüfung der Vergütungspflicht geeignet und erforderlich sein muss. Weitergehende Informationen über den Hergang einer Behandlung oder einer Operation sind im Gesetz nicht vorgesehen und für die Überprüfung der Rechnung auch nicht geeignet und erforderlich.

Im Rahmen der Wirtschaftlichkeitskontrolle wird das Verhältnis zwischen Kosten und Nutzen der angeordneten Massnahmen geprüft, wobei die Wirksamkeit vorausgesetzt wird. Die Wirtschaftlichkeitskontrolle wird stichprobenartig durchgeführt und dient allein zur Kontrolle der Leistungserbringer. Entsprechend müssten den Versicherern für diese Kontrollen auch anonymisierte Daten ausreichen. Nicht anonymisierte detaillierte Austritts- oder Operationsberichte sind somit weder geeignet noch erforderlich.

Urteil verschärft die Kontroverse

Das Bundesgericht erliess am 21. März 2007 ein Urteil, welches das Verhältnis zwischen Spital und Versicherer klären sollte (BGE 133 V 359). Das Bundesgericht hält darin fest, dass eine Versicherung selber über die erforderlichen Daten entscheiden könne. Die Heime, welche die Beschwerde angestrebt hatten, seien verpflichtet, diese Unterlagen herauszugeben.

PRIVATIM, die Vereinigung der Schweizerischen Datenschutzbeauftragten, hält in einer Stellungnahme zu diesem Urteil fest, dass auch im Rahmen einer Wirtschaftlichkeitsüberprüfung das Verhältnismässigkeitsprinzip gelte. Es dürfen somit nur jene Daten erhoben werden, die für die Überprüfung der Wirtschaftlichkeit objektiv erforderlich und geeignet sind. Die Haltung des Bundesgerichtes, wonach der Versicherer entscheiden kann, in welche Unterlagen er Einsicht nehmen will, ist für PRIVATIM schwer nachvollziehbar. PRIVATIM fordert, dass der Versicherer bekannt geben soll, welchen Inhalt und Umfang die Überprüfung hat. Gestützt darauf können die Leistungserbringer die Daten in der Regel sogar in anonymisierter Form weiterleiten. So würde auch das Berufsgeheimnis respektiert. PRIVATIM betont, dass Art. 42 KVG ein stufenweises Vorgehen ausdrücklich vorschreibe: Vorab genügt eine detaillierte und verständliche Rechnung. In Ausnahmefällen sind Zusatzinformationen erforderlich. Im Einzelfall darf der Leistungserbringer vom Versicherer erwarten, dass dieser mitteilt, welche Zusatzinformationen er wofür benötigt. In einem weiteren Schritt kann es in begründeten Fällen vorkommen, dass die Operations- und Austrittsberichte für die Überprüfung des Einzelfalles beigezogen werden müssen.

Klarer Handlungsbedarf

Im Oktober 2006 gelangte ein Bezirksspital an den Datenschutzbeauftragten mit der Frage, welche Haltung es gegenüber den Versicherern, die vollständige Austrittsberichte herausverlangen, einnehmen solle.

In der Folge bat der Datenschutzbeauftragte den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wiederholt, als Aufsichtsbehörde der Versicherer zu intervenieren. Der EDÖB verwies indessen darauf, dass ihn keine Behandlungspflicht treffe, und unternahm diesbezüglich bis heute nichts.

Die dargestellten Sachverhalte zeigen, dass nur die korrekte Anwendung der gesetzlichen Bestimmungen das Patientengeheimnis wahren kann. Doch Versicherer und eidgenössische Aufsichtsbehörden geben dem Schutz des Patientengeheimnisses nicht die notwendige Bedeutung.

Technisch möglich, rechtlich ungenügend

Technisch wird es in der Verwaltung in wenigen Jahren möglich sein, in grossem Ausmass personenbezogene Daten zentralisiert zu bearbeiten und innerhalb der Verwaltungsstellen und mit Privatpersonen auszutauschen. Über Einzelprojekte hinausgehende Sichtweisen und gesetzliche Regelungen sind nötig.

In der kantonalen Verwaltung besteht bereits ein Datenaustauschsystem mit Datenbank und -transportsystem. In den nächsten Jahren kommt eine Basisinfrastruktur für einheitliche Transaktionsmöglichkeiten hinzu. Diese wird auf einem harmonisierten Einwohnerregister aufbauen können. Ein solcher Datenpool wird tiefgreifende Auswirkungen auf die Privatheit der Bürgerinnen und Bürger haben.

Datenaustausch- und -transportsystem

Seit zehn Jahren betreibt die Abteilung Datenlogistik des Amtes für Raumordnung und Vermessung (ARV) eine Datenbank mit aktuellen Gebäudedaten, in welcher verschiedene Verwaltungsstellen ihre Daten erfassen. Dazu kommt ein Datentransportsystem. Alle angeschlossenen Stellen haben Zugriff auf die Datenbank. Das ARV wirbt dafür mit dem Slogan «Ein Datenbroker für die öffentliche Verwaltung». Die in den Datenpool aufzunehmenden Daten sowie die angeschlossenen Stellen können ohne weiteres erweitert werden.

Der Datenschutzbeauftragte bemängelte bereits in seinem 2. Tätigkeitsbericht 1996 die fehlenden gesetzlichen Grundlagen. Die in der Folge 1999 geschaffene Verordnung über geographische Daten und Informationssysteme in der kantonalen Verwaltung stellt keine genügende gesetzliche Regelung des Datenaustauschsystems dar. Ein erster Gesetzesentwurf 2003 war mangelhaft und wurde nicht weiterverfolgt. Ein neuer Anlauf zur Regelung der Datenlogistik wurde 2007 gestartet. Ende 2007 nahm sich auch die Geschäftsprüfungskommission des Kantonsrates der Thematik an; der Datenschutzbeauftragte legte gegenüber der Kommission den Regelungsbedarf dar.

Basisinfrastruktur für einheitliche Transaktionen

Die Stabsstelle E-Government bei der Staatskanzlei hat Ende 2007 die Submission für die Basisinfrastruktur für einheitliche, auf einem zentralen Personenstamm basierende Transaktionsmöglichkeiten für innerhalb der Verwaltung sowie für Privatpersonen und Unternehmen durchgeführt. Die projektierte Plattform ServicePortal baut auf der bestehenden Webinfrastruktur auf. Mittels der Plattform sollen diverse Datenbearbeitungen vorgenommen werden wie Authentisierung, Stammdatenverwaltung, Zwischenspeicherung vorab von Formulardaten, Datenübermittlung, Vorgangsverwaltung, Nutzungsstatistik sowie Rollen- und Benutzermanagement. Die Bearbeitung von besonders schützenswerten Personendaten ist nicht ausgeschlossen.

Der Datenschutzbeauftragte hatte in seiner Stellungnahme zum Grobkonzept deshalb festgehalten, es sei unabdingbar, dass vor der Inbetriebnahme des ServicePortals entsprechende rechtliche Grundlagen auf formell-gesetzlicher Ebene sowie Ausführungsbestimmungen geschaffen werden müssten. Die angestrebte Informationssicherheit sei zudem für die Bearbeitung von besonderen Personendaten nicht genügend.

Harmonisiertes Einwohnerregister

Die Volkszählung 2010 wird auf der Basis eines schweizweit einheitlichen Einwohnerregisters durchgeführt. Der Bund stellt eine zentrale Plattform – genannt Sedex – für den Datenaustausch zwischen den Personenregistern des Bundes und den kantonalen und kommunalen Einwohnerregistern sowie für die Datenlieferung an das Bundesamt für Statistik zur Verfügung. Der Datenschutzbeauftragte wird sich im Rahmen der Vernehmlassung zum kantonalen Registerharmonisierungsgesetz – der kantonalen Umsetzung der eidgenössischen Vorgaben – insbesondere damit auseinandersetzen, für welche Funktionen das bisher nur zu statistischen Zwecken bestehende virtuelle kantonale Einwohnerregister benutzt werden kann.

Im Rahmen der Registerharmonisierung soll eine neue, bei der Einwohnerkontrolle geführte Wohnungsnummer eingeführt werden; über diese kann der Bezug zur bestehenden, erweiterbaren Datenbank des ARV hergestellt werden.

Die projektierte Plattform für Transaktionen kann zudem mit Schnittstellen zum harmonisierten Einwohnerregister und zum Datentransportsystem ergänzt werden. Auf diese Weise wird technisch die Möglichkeit eröffnet, personenbezogene Daten in bisher nicht möglicher Art zentralisiert zu halten und zwischen verschiedenen Verwaltungsstellen untereinander sowie zwischen Privatpersonen und der Verwaltung auszutauschen.

Neue Möglichkeiten erfordern Gesamtschau

Die erwähnten Anwendungen und Projekte wurden und werden je separat geführt und beurteilt. Fragen nach rechtlichen Grundlagen, nach dem Verwendungszweck von personenbezogenen Daten, der Verhältnismässigkeit oder nach technischer Sicherheit werden deshalb nicht in einem Gesamtzusammenhang, sondern isoliert für das einzelne Vorhaben betrachtet.

Bereits bekannte oder durch Auswertung neu erzeugte Informationen werden zunehmend räumlich und zeitlich geordnet. Beispiele dafür sind Lageklasse der Liegenschaft, Eintrag im Altlastenverzeichnis, Bevölkerungsstruktur im Umkreis von 100 Metern oder Entfernung vom nächsten Eintrag in der Gefahrenkarte. Solche Informationen stellen personenbezogene Daten dar, können sie doch einem Grundeigentümer oder Mietenden oder auch einer Personen, die sich zu einer bestimmten Zeit an einem Ort aufgehalten hat, zugeordnet werden.

Werden eine Vielzahl solcher Informationen in einen Datenpool eingespeist, sind zahlreiche neuen Datenverknüpfungen möglich: Wohn- und Arbeitsorte von Personen, die an bestimmten Krankheiten verstorben sind, könnten beispielsweise mit Angaben über Altlasten, Produktionsstandorte bestimmter Stoffe und Luftbelastung verknüpft und Risikoprofile angelegt werden. Statistische Auswertungen werden inhaltlich wie auch örtlich immer mehr verfeinert.

Der Datenschutzbeauftragte weist darauf hin, dass aus einzeln betrachtet wenig bedeutungsvollen Informationen und statistischen Angaben besonders schützenswerte Personendaten entstehen können. Für die Bürgerinnen und Bürger hätte dies gravierende Folgen – von Versicherungsprämien über Grundstückspreise bis zur Quartierentwicklung. Er fordert deshalb eine Gesamtschau und gesetzliche Regelungen.

Fälle aus der Beratungstätigkeit

Einen Schwerpunkt der Tätigkeit des Datenschutzbeauftragten bildet die Beratungstätigkeit.

01.–19. ***Die hier zusammengefassten Fälle sind ausführlich dargestellt im Anhang auf Seite 25 ff. und auf der Website des Datenschutzbeauftragten (www.datenschutz.ch).***

01. **Einwohnerdatenbank nur für Statistik**
Das Statistische Amt schafft mit dem «Virtuellen Einwohnerregister für die Statistik» (Vesta) ein Einwohnerregister auf kantonaler Ebene. Sowohl das Statistische Amt als auch die Gemeinden dürfen die Daten jedoch nur für statistische Zwecke und nicht für Verwaltungszwecke verwenden.

02. **Sozialbehörden: Auskünfte an Gerichte**
Gemäss revidiertem Strafrecht sollen kurze Freiheitsstrafen möglichst durch Geldstrafen oder gemeinnützige Arbeit ersetzt werden. Sozialbehörden sind verpflichtet, Gerichten auf Anfrage Auskunft über die wirtschaftlichen Verhältnisse einer Person zu geben – und zwar ohne formelle Entbindung von der Schweigepflicht.

03. **Forschungsprojekt mit Jugendlichen**
In Forschungsprojekten müssen datenschutzrechtliche Vorgaben von Beginn weg berücksichtigt werden. Bei einem Forschungsprojekt über die Mediennutzung von Jugendlichen stellte der Datenschutzbeauftragte diverse datenschutzrechtliche Mängel fest.

04. **Merkblatt für Einwohnerkontrollen**
Ein Merkblatt des Datenschutzbeauftragten erläutert, ob und wie die Einwohnerkontrollen Personendaten bekannt geben und welche Regeln für die Aufbewahrung der Gesuche gelten.

05. **Wesensprüfung mit Hundehalterdaten**
Die Wesensprüfung eines Hundes entscheidet, ob ein Hund vom Leinen- und Maulkorbzwang befreit werden kann. Das Veterinäramt muss die Wesensprüfung dokumentieren. Bei der gefilmten Aufzeichnung darf auch der Hundehalter erfasst werden.

06. **Einsicht in Personalakten**
Die Geschäftsprüfungskommission des Kantonsrates (GPK) kann Einsicht in Amtsakten nehmen, sofern die Akten für die Aufgabenerfüllung der GPK geeignet und erforderlich sind. Auch Personalakten können unter dieses Einsichtsrecht fallen.

07. **Patientendaten an das kantonale Krebsregister**
Obwohl für das kantonale Krebsregister keine gesetzliche Grundlage besteht, können Spitäler im Kanton Zürich Patientendaten unter gewissen Einschränkungen an das kantonale Krebsregister weitergeben. Denn für Datenbearbeitungen zu nicht personenbezogenen Zwecken gelten erleichterte Voraussetzungen.

08. **Motionen zur Polizeidatenbank Polis**
Zwei Motionen der Geschäftsprüfungskommission des Kantonsrates (GPK) befassen sich mit der Polis-Datenbank und verlangen Verbesserungen in Bezug auf diese sensiblen Datenbearbeitungen.

09. **Entsorgte Akten bleiben vertraulich**
Um vertrauliche Akten zur Vernichtung zu sammeln, werden in Ämtern oft speziell gesicherte Sammelcontainer bereitgestellt. Wie bei einem Aktenschredder dürfen eingeworfene Akten nicht mehr herausgenommen werden können – auch nicht bei versehentlichem Einwurf.

10. **Weltanschauung von Erwerbslosen**
Ein Verein integriert im Auftrag eines Sozialamts Erwerbslose in eine Erwerbstätigkeit. Sein Bericht an das Sozialamt enthielt Aussagen über die Erwerbslosen, die keinen Bezug zum Arbeitsverhältnis hatten. Ein Arbeitnehmer, der damit nicht einverstanden ist, kann eine Berichtigung verlangen.

11. **Merkblatt für Sozialinspektoren**
Wenn ein Verdacht auf Sozialhilfemissbrauch besteht, können Sozialämter Sozialinspektoren einsetzen. Zur Klärung der datenschutzrechtlichen Rahmenbedingungen bei solchen Einsätzen hat der Datenschutzbeauftragte ein Merkblatt verfasst.

12. **Einzel-, Listenauskünfte und Webpublikation**
Öffentliche Organe können Personendaten an Privatpersonen bekannt gegeben, wenn dafür gesetzliche Grundlagen bestehen. Für Auskünfte im Einzelfall, Listenauskünfte sowie für eine Publikation im Amtsblatt oder im Internet gelten unterschiedliche Regelungen.

13. **Datenschutzgesetz und Aufsichtsbeschwerde**
Obwohl das Datenschutzgesetz in Verfahren der Verwaltungsrechtspflege nicht anwendbar ist, gilt es bei der Behandlung von Aufsichtsbeschwerden. So auch im konkreten Fall, in dem im Rahmen einer Aufsichtsbeschwerde ein Bezirksrat von einem Amt Angaben über fehlbare Bauern einverlangte.

14. **Eignungsabklärung für bestimmte Berufe**
Für eine Berufsausbildung in Pädagogik- oder Gesundheitsberufen wird abgeklärt, ob sich jemand dafür auch eignet. Daten, die im Rahmen von Eignungstests erhoben und weitergeleitet werden, müssen in jedem einzelnen Fall für den jeweiligen Abklärungszweck unentbehrlich sein.

15. **Videoübertragung als Datenbearbeitung**
Eine Live-Übertragung mittels Videokameras auf Monitore fällt in den Geltungsbereich des Datenschutzgesetzes – auch wenn die übertragenen Daten nicht aufgezeichnet werden.

16. **Meldepflicht für ausländische Sozialhilfebezüger**
Das neue Ausländergesetz führt die Meldepflicht für sozialhilfeabhängige Ausländerinnen und Ausländer ein. Gemeinden, die Sozialhilfe zahlen, müssen das Migrationsamt über Beginn, Umfang und Beendigung eines Sozialhilfebezugs informieren.

17. **Kostengutsprache braucht keine Diagnose**
Für eine Kostengutsprache nach einer unvorhergesehenen Spitalbehandlung darf das Sozialamt nur nach den Gesundheitsdaten fragen, die für die Anspruchsabklärung geeignet und erforderlich sind. Anstelle einer medizinischen Diagnose reicht dazu eine Umschreibung der Behandlungsursache.

18. **Skilager mit Folgen für die Schulpflege**
Die Schulpflege einer Primarschule führte ein Skilager durch. Während des Lagers kam es zu teilweise strafrechtlich relevanten Vorfällen ohne Nachweis der Täterschaft. Die Bekanntgabe der Namen der Verdächtigen an alle Eltern und die Sekundarstufe war weder gesetzes- noch verhältnismässig.

19. **Fachgutachter im Beschwerdeverfahren**
Im Beschwerdeverfahren sind Beschwerdeinstanzen grundsätzlich an die Feststellungen des Datenschutzbeauftragten gebunden.

Case Management im Personalwesen

Das Case Management wurde auf die ganze kantonale Verwaltung ausgeweitet. Im Rahmen des Vernehmlassungsverfahrens wies der Datenschutzbeauftragte erneut darauf hin, dass die datenschutzrechtlichen Anforderungen in mehreren Punkten nicht erfüllt werden.

Die Direktion der Justiz und des Innern (JI) führte in den vergangenen Jahren ein Pilotprojekt Case Management mit dem Namen «Reha-Unterstützung» durch (vgl. Tätigkeitsbericht Nr. 10 [2004]). Im Rahmen des Vernehmlassungsverfahrens vom ersten Quartal 2007 über die Ausweitung des Case Management auf die ganze kantonale Verwaltung bezog der Datenschutzbeauftragte erneut Stellung.

Gesetzliche Grundlage

Der Datenschutzbeauftragte wies wiederholt darauf hin, dass die im Rahmen des Case Management erhobenen Daten besonders schützenswerte Personendaten darstellen (§ 2 lit. d DSG, künftig: besondere Personendaten i.S.v. § 3 IDG). Die Bearbeitung dieser Daten bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz (§ 5 lit. a DSG; § 8 Abs. 2 IDG). Die Bekanntgabe darf nur aufgrund einer hinreichend bestimmten Regelung in einem formellen Gesetz erfolgen (§ 5 lit. a DSG; § 17 lit. a IDG).

Im Weiteren legte der Datenschutzbeauftragte dar, dass gemäss § 55 des Personalgesetzes (PG) Mitarbeitende wohl verpflichtet werden können, sich einer Untersuchung durch einen – vom Regierungsrat gewählten und von der BVK im Einzelfall bestimmten – Vertrauensarzt zu unterziehen. § 55 PG ist jedoch keine genügende gesetzliche Grundlage für die Einsetzung eines Case Manager oder für die Verpflichtung der Mitarbeitenden zur Zusammenarbeit mit diesem.

Eine Regelung auf Verordnungsbasis, wie dies in der Vernehmlassungsvorlage vorgesehen war und inzwischen durch Änderung der §§ 100a und 103 der Vollzugsverordnung zum Personalgesetz (VVO PG) umgesetzt worden ist, genügt den aufgezeigten Anforderungen der formellen gesetzlichen Grundlage nicht. Vielmehr sind in einem formellen Gesetz die Aufgaben, Kompetenzen sowie die Verantwortung eines Case Manager und die damit zusammenhängenden Datenbearbeitungen zu umschreiben. Ausdrücklich zu regeln sind auch die Aufbewahrung und der Zugriff auf die Akten des Case Management.

Einwilligung der betroffenen Person

In der Stellungnahme wurde auch darauf hingewiesen, dass eine fehlende gesetzliche Grundlage für eine Datenbearbeitung im Einzelfall durch die Einwilligung der betroffenen Person ersetzt werden kann (§ 5 lit. c DSG). In weiterer Auslegung dieser Bestimmung sind zeitlich und personell begrenzte, auf dem Grundsatz der Freiwilligkeit basierende Pilotversuche möglich. Eine definitive Einführung bedarf aber in jedem Fall der skizzierten Regelungen in einem Gesetz im formellen Sinn.

Entbindung von der beruflichen Schweigepflicht

Weiter muss die Verletzung des Berufsgeheimnisses nach Art. 321 StGB berücksichtigt werden: Medizinalpersonen unterstehen der beruflichen Schweigepflicht über alle Kenntnisse, die ihnen im Rahmen ihres Berufes von den Mitarbeitenden anvertraut worden sind oder die sie in dessen Ausübung wahrgenommen haben (Art. 321 Ziff. 1 Abs. 1 StGB) – und zwar unabhängig davon, wer sie beauftragt hat. Der Case Manager ist grundsätzlich keine Hilfsperson, welche der Schweigepflicht unterstehen würde; allenfalls kann eine Medizinalperson als Case Manager eingesetzt werden.

Die Schweigepflicht kann im vorliegenden Fall nur durch Einwilligung des Mitarbeiters aufgehoben werden.

Auch die Einführung des Case Management in der kantonalen Verwaltung mittels §§ 100a und 103 VVO PG ändert nichts an der geltenden Rechtslage, wonach für Mitarbeitende keine Pflicht besteht, Medizinalpersonen von der beruflichen Schweigepflicht zu entbinden. Genauso wenig können Mitarbeitende verpflichtet werden, den Grund einer Erkrankung oder eine ärztliche Diagnose Vorgesetzten, dem Case Manager oder Dritten mitzuteilen.

Outsourcing

Wie dies im Vernehmlassungsentwurf vorgesehen war und mit geltender Regelung in Kraft gesetzt worden ist, wird das Case Management Dritten übertragen. In der Stellungnahme wurde darauf hingewiesen, dass die datenschutzrechtlichen Vorgaben durch Auflagen, Vereinbarungen oder auf andere geeignete Weise sicherzustellen seien (§ 13 DSG, § 6 IDG).

Gegenüber den im Einzelfall eingesetzten Case Managers ist ein fachliches Weisungsrecht des beauftragenden öffentlichen Organs zu vereinbaren, um das Amtsgeheimnis auf diese zu überbinden. Die ergänzende vertragliche Schweigepflicht ist mit einer Konventionalstrafe abzusichern. Eine gesetzlich statuierte Geheimhaltungspflicht für Case Managers ist wünschenswert, um unzulänglich geregelte Einzelverträge zu vermeiden.

Damit schliesslich die Einhaltung der datenschutzrechtlichen Anforderungen für alle Case-Management-Betreuungen einheitlich sichergestellt werden kann, soll der Regierungsrat verbindlich allgemeine Geschäftsbedingungen als Bestandteil aller Case-Management-Verträge formulieren. Alternativ könnten solche Rahmenbedingungen auch in der VVO PG festgesetzt werden.

Die datenschutzrechtlichen Anforderungen werden nun teilweise erfüllt. Das Case Management wird per 1. April 2008 durch Beschluss des Regierungsrates eingeführt.

Verordnung zum IDG

Ein erster Entwurf der Verordnung über die Information und den Datenschutz enthielt zahlreiche gelungene Bestimmungen in Bezug auf den Datenschutz. In der Vernehmlassung wurden jedoch die fehlenden Bestimmungen zur Konkretisierung des Öffentlichkeitsprinzips kritisiert.

Im Dezember 2006 setzte die Direktion der Justiz und des Innern (JI) eine Arbeitsgruppe mit dem Auftrag ein, einen Vorentwurf der Verordnung zum Gesetz über die Information und den Datenschutz (IDG) auszuarbeiten. In dieser Arbeitsgruppe wirkte auch der Datenschutzbeauftragte mit.

Der Vorentwurf wurde am 26. Juni 2007 zur breiten Vernehmlassung gestellt. Er enthielt folgende Konkretisierungen des Gesetzes in Bezug auf den Datenschutz: Das Vorgehen bei Forschungsprojekten und bei der Auftragserteilung an Dritte wurde mit den notwendigen Leitlinien versehen. Auch die im Gesetz neu eingeführte Vorabkontrolle wurde mit dem erforderlichen Rahmen versehen. Weitere Bestimmungen konkretisierten den Umgang mit besonderen Personendaten, die Qualitätssicherung, das Auskunftsrecht, das Sperren von Personendaten sowie die Konsequenzen, wenn eine vom Datenschutzbeauftragten ausgesprochene Empfehlung nicht befolgt wird.

Der Datenschutzbeauftragte erachtete den Vorentwurf in Bezug auf den Datenschutz gesamthaft als gelungen und regte in seiner Stellungnahme nur marginale Änderungen an. In der Vernehmlassung wurden jedoch zahlreiche Einwände erhoben, vorab im Zusammenhang mit der Umsetzung des Öffentlichkeitsprinzips. Die JI nahm deshalb eine grundlegende Überarbeitung vor.

Weitere Schritte für mehr Sicherheit

Zusätzlich zu seiner Kontrolltätigkeit erarbeitete der Datenschutzbeauftragte gemeinsam mit ausgewählten Fachstellen die notwendigen Grundlagen für ein vereinfachtes Vorgehen bei der Umsetzung von Sicherheitsmassnahmen für Amtsstellen und Gemeinden – sowie weitere Hilfsmittel zur Sicherheit im Informatikbereich.

Der Datenschutzbeauftragte überprüfte ausgewählte Stellen innerhalb der kantonalen Verwaltung, Spitäler und Kliniken, Fachhochschulen, Statthalterämter und Gemeinden. Den Schwerpunkt der Kontrollen bildeten auch in der Berichtsperiode die Gemeinden und ihre Dienstleistenden sowie die regionalen Informatikzentren (siehe Kasten auf Seite 20). Die Prüfungen erfolgten im gleichen Umfang und mit dem gleichen Massstab wie in den Vorjahren.

Dass der Datenschutzbeauftragte die kantonalen Stellen in Zusammenarbeit mit der Finanzkontrolle prüfte, erwies sich für beide Seiten als Vorteil: Das koordinierte Vorgehen ermöglichte vertiefte Kontrollen und war für die Amtsstellen mit einem geringeren Zeitaufwand verbunden. Dabei wurden folgende Themen geprüft:

- Sicherheitsstrategie oder -leitlinie:
  Die geprüften Stellen sind häufig nicht mit den eigenen Sicherheitszielsetzungen vertraut und haben oft keine geeignete Organisation im Bereich ICT-Sicherheit. Fehlen klare Sicherheitsziele, ist der Umfang der zu ergreifenden Massnahmen für ein angemessenes Niveau der ICT-Sicherheit unklar und eine Priorisierung der Ressourcen nicht möglich.
- Information Security Management Systems (ISMS):
  Die grösseren Stellen mit einem komplexen Umfeld verfügen mit wenigen Ausnahmen über kein Sicherheits-Managementsystem (nach den Standards BSI 100-1 oder ISO/IEC 27001). Erst der Einsatz solcher Kontrollmechanismen stellt einheitliche Anforderungen an die verwalteten Systeme und Applikationen und ermöglicht ein frühzeitiges Erkennen von Lücken.
- Mobile Arbeitsplätze und Geräte:
  Trotz zunehmender Ausbreitung von mobilen Geräten wie Personal Digital Assistants (PDA) sind sowohl die Weisungen an das Personal als auch entsprechende technische Massnahmen (beispielsweise im kryptografischen Bereich) noch selten anzutreffen. Dabei sind solche Massnahmen die Voraussetzung für eine gelebte Sicherheitskultur in den Stellen.
- Rollen- und Berechtigungskonzept:
  Entsprechende Vorarbeiten in Form einer Zugriffsmatrix über die Datei- und Applikationssysteme sind zwar meistens vorhanden, das Wissen über das Regelwerk im Detail und als Gesamtübersicht in den Rollen hat aber nur der ICT-Verantwortliche, oft ohne schriftlichen Aufzeichnungen. Mit der kurzen Dokumentation, die der Datenschutzbeauftragte bereits seit mehreren Jahren als Hilfestellung anbietet, kann mit minimalem Aufwand die erforderliche Transparenz geschaffen werden zwischen den bereits eingerichteten Definitionen für die Dateneigentümer als Auftraggeber und dem internen und dem externen ICT-Personal als ausführende Stelle.
- Zusammenarbeit mit externen Supportstellen:
  Oft fehlen Vorgaben und Leitplanken für die Detailarbeiten (Umfang der Betriebsdokumentationen, Umfang und Periodizität von Auswertung, Meldewege und im Voraus festgelegte Aktionen bei sicherheitsrelevanten Vorfällen etc.). Um sicherzustellen, dass die externen Dienstleistenden das ICT-Sicherheitskonzept und dessen Massnahmen auch pflichtgemäss umsetzen, müssen solche Vereinbarungen regelmässig überprüft werden.
- Aufbewahrungsfristen:
  Meistens wurden die Aufbewahrungsfristen gemäss §14 Abs. 2 DSG nicht festgelegt.

Die finanziellen und insbesondere die personellen Ressourcen zur Umsetzung eines vernünftigen ICT-Sicherheitsniveaus sind grösstenteils immer noch zu knapp bemessen. Der Datenschutzbeauftragte

fordert seit Jahren, dass die Mittel für die organisatorischen und technischen Massnahmen so eingesetzt werden, dass ein angemessenes Sicherheitsniveau gefestigt und ausgebaut werden kann. Diese Prioritätenverschiebung hat in der Berichtsperiode noch nicht stattgefunden.

Mitarbeit in Arbeitsgruppen

Mit der Teilnahme und aktiven Mitarbeit in Arbeitsgruppen, in die kantonale und kommunale Vertreter involviert sind, kann der Datenschutzbeauftragten seine beschränkten Ressourcen in Hauptthemen der ICT-Sicherheit mit dem grössten Multiplikatoreffekt einsetzen.

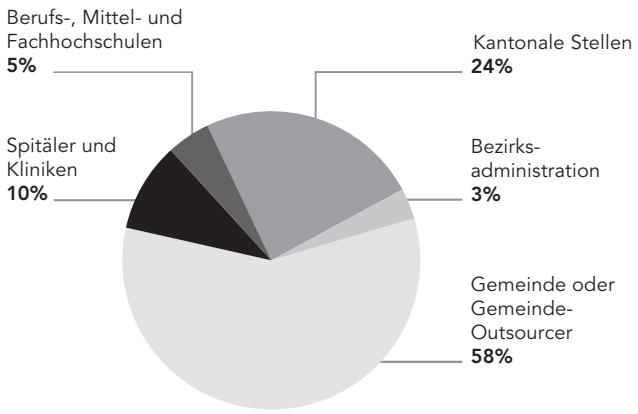
In der Arbeitsgruppe ZH171 hat sich

Datenschutzreviews 1.1.2000–31.12.2007

Geprüfte Stellen 2000 bis 2007

Der Datenschutzbeauftragte prüfte von 2000 bis 2007 62 Stellen

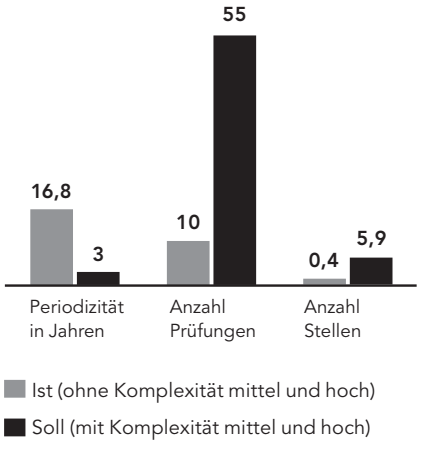
Durchgeführte Prüfungen	Anzahl
Kantonale Stellen	15
Bezirksadministration	2
Gemeinde oder Gemeinde-Outsourcer	36
Spitäler und Kliniken	6
Berufs-, Mittel- und Fachhochschulen	3



Soll-Ist-Vergleich von Periodizität, Anzahl Prüfungen pro Jahr und Anzahl Stellen

Prüfungsintervall der zu prüfenden Stellen:

Total 266 Stellen, davon 168 mit Priorität ausgewählt:	
32	Kantonale Stellen mit eigenem IT-Personal
12	Bezirksverwaltungen
171	Gemeinden (73 ausgewählt für Kontrolle) und 2 Outsourcer
6	Spitäler und Kliniken
45	Berufs-, Mittel- und Fachhochschulen



der Datenschutzbeauftragte zusammen mit Teilnehmenden aus dem kantonalen IT-Team (KITT) und Vertretern der Interessengemeinschaft IG EDV mit der Netzwerksicherheit der Gemeinden innerhalb des kantonalen Gesamtnetzes LEUnet befasst. Schwerpunkte bildeten 2007 die Network Security Policy (NSP) des Netzwerks GELB-Gemeinden und ihrer detaillierten Anhänge, die Vorgehensweise für die Anbindung der Gemeinden an die NSP mittels Verträgen und die Klärung zahlreicher Detailaspekte.

In der 2006 gebildeten Arbeitsgruppe «Methoden und Standards» erarbeitete der Datenschutzbeauftragte mit der Finanzkontrolle und den Revisionsdiensten des Gemeindeamts gemeinsame kantonsinterne Standards und Vorgehensweisen für die Bereiche der organisatorischen und technischen Hilfsmittel. So wurde der Schutzbedarf der Gemeinden und Amtsstellen festgelegt, Softwarescanner zur Prüfungsunterstützung wurden evaluiert oder Beispiele für eine IT-Sicherheitspolitik und -Sicherheitsleitlinie erarbeitet. Die Arbeitsgruppe entwickelte zudem eine methodische Vorgehensweise für ICT-Sicherheitskonzepte, die vollständig in die Umsetzungshilfe ICT-Sicherheit übernommen wurde.

Unterstützung für ICT-Sicherheit

Der Datenschutzbeauftragte hat 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 Umsetzungshilfe soll den Gemeinden und Amtsstellen ein möglichst einfaches Verfahren zur Umsetzung von ICT-Sicherheit ermöglichen. Von den ICT-Verantwortlichen soll es ohne grosses Know-how und mit bescheidenen Ressourcen sofort eingesetzt werden können. Bereits vorhanden sind für Amtsstellen und Gemeinden

- Klassifizierungshilfen für die Sicherheitsstufe nach ISV und nach Komplexitätsgrad
- ICT-Strukturanalyse (vorerst für Gemeinden)
- Schutzbedarfsfeststellung
- Modellierung des ICT-Verbundes
- Massnahmenlisten N1 und N2 als Minimumstandard, basierend auf dem BSI-Grundschutzkatalog

Die Ergebnisse können später, wie geplant, in das Softwareprodukt GSTOOL des Bundesamts für Sicherheit in der Informationstechnik (BSI) übernommen und von den Stellen weiterbearbeitet werden. Der Datenschutzbeauftragte hat die Definitionen bereits vorgefertigt; die Amtsstellen und Gemeinden sind dadurch von der Definitionsphase befreit und können direkt den Massnahmenplan erstellen und später umsetzen. Weitere Hilfestellungen für die Stellen wie die Vorgabe einer Sicherheitsleitlinie und -politik sowie ein Rollen- und Zugriffskonzept wurden 2007 vom Datenschutzbeauftragten neu erstellt oder aktualisiert.

Ausblick

Dank den Vorarbeiten für die Umsetzungshilfe für ICT-Sicherheit werden die kantonalen Amtsstellen, Bezirksverwaltungen und Gemeinden ein Werkzeug erhalten, das an ihre Ressourcen angepasst ist. Die Resultate in der Berichtsperiode zeigen deutlich, dass die Datenschutzreview als Standardkontrolle des Datenschutzbeauftragten als Prüfungs- und Sensibilisierungsinstrument weiterhin dringend notwendig ist.

Neuer Schwerpunkt Kommunikation

Um die Bevölkerung für den Wert der Privatheit zu sensibilisieren, die datenbearbeitenden Stellen zu unterstützen sowie als Reaktion auf die wachsende Nachfrage nach Datenschutzinformationen verstärkt der Datenschutzbeauftragte seine Kommunikation – ergänzt durch Weiterbildung und Kooperationen.

Die Technologie gefährdet zunehmend das Grundrecht auf Privatheit. Datenschutzbeauftragte allein können den Schutz der Privatheit nicht garantieren. Zu gering sind ihre Einflussmöglichkeiten. Umso vordringlicher wird es für sie, die Öffentlichkeit für den Wert der Privatheit zu sensibilisieren. Das Datenschutzgesetz fokussiert deshalb nicht nur auf sichere Technologie, sondern auch auf Information und Sensibilisierung der Bürgerinnen und Bürger.

Gleichzeitig hat die Nachfrage nach Informationen zum Thema Datenschutz in den letzten Jahren stark zugenommen: Die Medien greifen vermehrt Aspekte des Datenschutzes auf – meistens im Zusammenhang mit aktuellen Vorkommnissen – und wenden sich dabei zunehmend auch an den Datenschutzbeauftragten. Auch die Nachfrage nach Gastreferaten des Datenschutzbeauftragten an verschiedenen, auch internationalen Veranstaltungen ist in den letzten Jahren deutlich gestiegen.

Informieren und sensibilisieren

Mit Blick auf neue Aufgaben und Herausforderungen hat der Datenschutzbeauftragte das Gewicht seiner Tätigkeiten etwas verlagert: Neben Aufsicht und Kontrolle sowie Beratung und Vermittlung für Bürgerinnen und Bürger bildet die Kommunikation einen neuen Schwerpunkt.

Anfang 2007 besetzte der Datenschutzbeauftragte eine offen gewordene Stelle mit einer Kommunikationsspezialistin (50%). Kommunikationskonzepte für die verwaltungsinterne und für die externe Kommunikation sind nun erarbeitet. Im Rahmen der begrenzten Möglichkeiten werden jetzt vordringliche Aspekte des Datenschutzes noch aktiver und zielgruppengerecht kommuniziert, wie folgende Beispiele aus der Berichtsperiode zeigen:

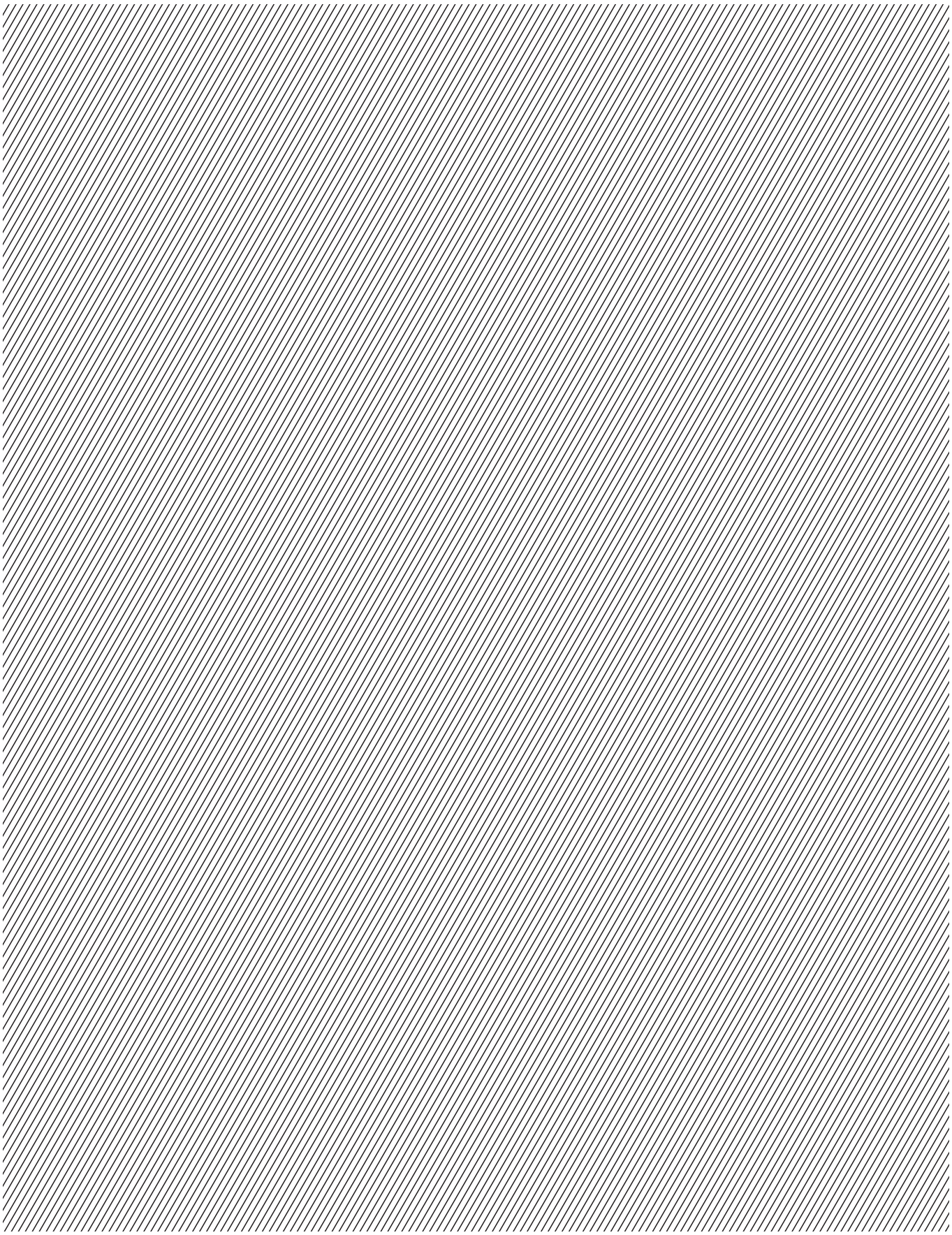
- Die Broschüre «Ihr Patientendossier – Ihre Rechte» wurde für die Zürcher Spitäler zur Abgabe an die Patientinnen und Patienten erstellt.
- Die stets aktuelle Website des Datenschutzbeauftragten enthält Hilfestellungen wie Musterbriefe für Bürgerinnen und Bürger und juristische Praxisbeispiele für Fachleute (www.datenschutz.ch).
- Merkblätter für die Einwohnerkontrolle oder für die Sozialämter geben Handlungsanleitungen in ausgewählten Bereichen und ermöglichen eine einheitliche Praxis.

Die Sensibilisierung all jener Personen, die speziell Personendaten bearbeiten, ist für den Datenschutzbeauftragten vordringlich: Mit einem gezielten Aus- und Weiterbildungsangebot befähigt er sie, den Datenschutz selbständig in ihrem Wirkungskreis sicherzustellen. So wurden auch vier neue Module für Verwaltungsangestellte konzipiert: ein Update für Juristinnen und Juristen sowie Seminare für Informatikfachleute, für das Sozialwesen und für das Gesundheitswesen. Die Seminare wurden im Rahmen der kantonalen Aus- und Weiterbildung angeboten.

Synergien durch Vernetzung

Zentrale Themen des Datenschutzes wie das Patientengeheimnis, die Umsetzung der Abkommen von Schengen/Dublin und Videoüberwachung betreffen nicht nur die Bürgerinnen und Bürger im Kanton Zürich. Deshalb führte der Datenschutzbeauftragte Medienorientierungen zu diesen Themen gemeinsam mit PRIVATIM, der Vereinigung der schweizerischen Datenschutzbeauftragten, durch – sowie ein Fachseminar für Medienschaffende. Durch die Zusammenarbeit mit PRIVATIM konnte eine grössere Wirkung bei gleichzeitigem Synergiegewinn erreicht werden. Im Rahmen dieser schweizweiten Vernetzung übernahm PRIVATIM die Patientendossier-Broschüre des Datenschutzbeauftragten (s.o.) und gibt sie nun in drei Sprachen an die Kantone ab.

In Zusammenarbeit mit der Stiftung für Datenschutz und Informationssicherheit veranstaltete der Datenschutzbeauftragte die Symposien «Pay as you drive und Persönlichkeitsschutz» sowie das 12. «Symposium on Privacy and Security 2007» zum Thema «Datenschutz und Informationssicherheit in die Prozesse integrieren». Die Symposien richteten sich an Entscheidungsträger aus Wirtschaft, Verwaltung und Politik und fanden grossen Anklang.



Fälle aus der Beratungstätigkeit
Anhang

Titel: Einwohnerdatenbank nur für Statistik
URL: http://www.datenschutz.ch/themen/1336.php
Datum: 26.08.2008

01.

Einwohnerdatenbank nur für Statistik

Das Statistische Amt schafft mit dem «Virtuellen Einwohnerregister für die Statistik» (Vesta) ein Einwohnerregister auf kantonaler Ebene. Sowohl das Statistische Amt als auch die Gemeinden dürfen die Daten jedoch nur für statistische Zwecke und nicht für Verwaltungszwecke verwenden.

Im Rahmen des Projekts «Virtuelles Einwohnerregister für die Statistik» (Vesta) erarbeitet das Statistische Amt eine kantonsweite Datenbank, um Statistiken erstellen zu können. Mit dem Virtuellen Einwohnerregister sollen Daten über Einwohner, Alter, Wanderung und Leerwohnungen erhoben und die Einwohnerregister harmonisiert werden.

Das Statistische Amt wandte sich für eine Stellungnahme zum Projekt Vesta an den Datenschutzbeauftragten. Es war in erster Linie abzuklären, ob die erforderlichen gesetzlichen Grundlagen vorlagen, welche die Datenbekanntgabe von den Gemeinden an das Statistische Amt ermöglichen.

Mit Inkraftsetzung des Bundesgesetzes über die Registerharmonisierung per 1. November 2006 wurden diese geschaffen. Das Gesetz listet diejenigen Personendaten auf, welche die Einwohnerkontrollen der Gemeinden für die Registerharmonisierung zu erheben verpflichtet sind. Der Merkmalskatalog von Vesta wiederholt lediglich diese Liste.

Im Projekt Vesta sind die Gemeinden für die Modalitäten der Datenbekanntgabe an das Statistische Amt verantwortlich. Sie haben die Datenherrschaft über alle Daten, die sie manuell, halbautomatisch und automatisch übermitteln. Die Gemeinden haben dabei die technischen Datenschutzvorgaben einzuhalten und Daten somit immer verschlüsselt und authentisiert zu übermitteln. Der Transportweg der Exportdaten wird vom Statistischen Amt automatisch festgelegt. Das Statistische Amt trägt auch die Verantwortung für die Systeminfrastruktur des gesamten Projekts Vesta.

Der Datenschutzbeauftragte gelangte zum Schluss, dass dem Projekt Vesta aus Sicht des Datenschutzes nichts entgegensteht, weil die Daten ausschliesslich zu statistischen Zwecken Verwendung finden.

Titel: Sozialbehörden: Auskünfte an Gerichte
URL: http://www.datenschutz.ch/themen/1337.php
Datum: 26.08.2008

02.

Sozialbehörden: Auskünfte an Gerichte

Gemäss revidiertem Strafrecht sollen kurze Freiheitsstrafen möglichst durch Geldstrafen oder gemeinnützige Arbeit ersetzt werden. Sozialbehörden sind verpflichtet, Gerichten auf Anfrage Auskunft über die wirtschaftlichen Verhältnisse einer Person zu geben – und zwar ohne formelle Entbindung von der Schweigepflicht.

Ein Gericht benötigte für eine Hauptverhandlung Angaben zu den wirtschaftlichen Verhältnissen eines Angeklagten, der Sozialhilfe bezog. Die zuständige Sozialbehörde erteilte die für die Strafzumessung wesentlichen Informationen zu spät, nämlich erst nach dem Prozess und erst nachdem die fallverantwortliche Sozialarbeiterin von ihrer vorgesetzten Stelle vom Amtsgeheimnis entbunden worden war.

Im Lichte des neuen Art. 34 Abs. 3 StGB empfand das Gericht das Vorgehen der Sozialbehörde als unnötig langwierig und kompliziert. Der Gerichtspräsident bat den Datenschutzbeauftragten um eine Beurteilung der Rechtslage.

Mit der Revision des Strafrechts sollen kurze Freiheitsstrafen möglichst durch Geldstrafen oder gemeinnützige Arbeit ersetzt werden. Die individuell zugemessenen Geldstrafen können bis zu 360 Tagessätze betragen (Art. 34 Abs. 1 StGB). Die Höhe der einzelnen Tagessätze bestimmt sich nach den persönlichen und wirtschaftlichen Verhältnissen des Täters im Zeitpunkt des Urteils, namentlich nach Einkommen und Vermögen, Lebensaufwand, allfälligen Familien- und Unterstützungspflichten, sowie nach dem Existenzminimum (Art. 34 Abs. 2 StGB). Für die Bemessung der Tagessätze sind die Gerichte auf Auskünfte von Behörden des Bundes, der Kantone und der Gemeinden angewiesen.

Aufgrund der neuen Bestimmungen sind die Sozialbehörden verpflichtet, einer anfragenden gerichtlichen Behörde Auskunft über die finanziellen Verhältnisse einer verurteilten Person zu erteilen (Art. 34 Abs. 3 StGB). Dabei hat die Sozialbehörde unter Anwendung des Verhältnismässigkeitsprinzips zu beachten, dass nur diejenigen Personendaten aus den in Art. 34 Abs. 2 StGB genannten Daten weitergeleitet werden, die für die Bemessung der Tagessätze geeignet und erforderlich sind. Eine formelle behördliche Entbindung von der Schweigepflicht ist nicht notwendig.

Titel: Forschungsprojekt mit Jugendlichen
URL: http://www.datenschutz.ch/themen/1338.php
Datum: 26.08.2008

03.

Forschungsprojekt mit Jugendlichen

In Forschungsprojekten müssen datenschutzrechtliche Vorgaben von Beginn weg berücksichtigt werden. Bei einem Forschungsprojekt über die Mediennutzung von Jugendlichen stellte der Datenschutzbeauftragte diverse datenschutzrechtliche Mängel fest.

Im Rahmen einer Dissertation befragte ein Doktorand verschiedene Schulklassen zu ihrer Mediennutzung. Der dazu erarbeitete Fragebogen enthielt vor allem Fragen, wie die Jugendlichen unterschiedliche Medien nutzen. Einzelne Fragen zielten aber auch auf die «interpersonale Kommunikation», den Suchmittelkonsum sowie auf Sympathiewerte gegenüber den Mitschülerinnen und Mitschülern. Der Fragebogen konnte sowohl auf Papier als auch übers Internet ausgefüllt werden.

Die Mutter einer Schülerin fragte den Datenschutzbeauftragten, ob diese Erhebung zulässig sei. Die Abklärungen des Datenschutzbeauftragten deckten verschiedene datenschutzrechtliche Mängel in der wissenschaftlichen Untersuchung auf. So wurden zwölfjährige Schülerinnen und Schüler ohne Einwilligung des gesetzlichen Vertreters in die Studie einbezogen. Das Recht der informationellen Selbstbestimmung ist ein verfassungsmässiges Recht. Soweit Jugendliche unter 18 Jahren urteilsfähig sind, können sie dieses Recht selbst ausüben (Art. 19 Abs. 2 Zivilgesetzbuch). Die Urteilsfähigkeit ist aber erst ab etwa 14 Jahren vorauszusetzen. Werden Zwölfjährige in eine solche Untersuchung involviert, müssen die Erziehungsberechtigten der Befragung zustimmen.

Zu wenig beachtet wurde der Aspekt der Freiwilligkeit: Auf den Fragebögen fehlte ein klarer Hinweis, dass die Teilnahme an der Untersuchung freiwillig sei. Bei Schülerinnen und Schülern, welche die Fragen nicht beantwortet hatten, wurde zudem wiederholt nachgehakt. Schliesslich wurde in Aussicht gestellt, unter jenen Klassen, in welchen alle Schülerinnen und Schüler an der Befragung teilnehmen würden, Kinogutscheine zu verlosen. Der Datenschutzbeauftragte konstatiert, dass insgesamt zu grosser Druck zur Teilnahme auf die Jugendlichen ausgeübt wurde. Die Bekanntgabe von Personendaten für ein Forschungsprojekt muss auf freiem Willen basieren.

Im Forschungsprojekt wurde die Informatiksicherheit zu nachlässig gehandhabt: Daten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (§ 4 Abs. 5 DSG). Im Forschungsprojekt wurden jedoch die besonders schützenswerten Personendaten unverschlüsselt übers Internet übermittelt. Die Website wurde ausserdem nicht von der Hochschule, sondern von einem Dritten betrieben. Der Vertrag mit diesem Provider enthielt keinerlei Bestimmungen zum Datenschutz, zu Sicherheitsstandards oder zu Haftungsregelungen.

Nach Intervention des Datenschutzbeauftragten wurden die datenschutzrechtlich unzureichenden Punkte des Forschungsprojekts korrigiert.

Titel: Merkblatt für Einwohnerkontrollen
URL: http://www.datenschutz.ch/themen/1339.php
Datum: 26.08.2008

04.

Merkblatt für Einwohnerkontrollen

Private Personen und Organisationen können der Einwohnerkontrolle Gesuche für die Bekanntgabe von Personendaten stellen. Ein Merkblatt des Datenschutzbeauftragten erläutert, ob und wie die Einwohnerkontrollen die Daten bekannt geben und welche Regeln für die Aufbewahrung der Gesuche gelten.

Der Datenschutzbeauftragte wurde von Einwohnerkontrollen immer wieder angefragt, wie Auskunftsgesuchen von privaten Personen und Organisationen nachzukommen sei und wie lange diese Gesuche aufbewahrt werden müssten. Er hat deshalb das Merkblatt «Einwohnerkontrolle: Auskunftsrecht und Gesuchsaufbewahrung» erarbeitet, das diese Fragen klärt:

Private, die sich ausgewiesen haben, können bei der Einwohnerkontrolle Gesuche für die Bekanntgabe von Personendaten stellen. Die Bekanntgabe erfolgt gemäss § 9 DSG auf verschiedene Arten.

Je nachdem, welche Daten gewünscht werden oder ob eine Datensperre besteht, gelten für die Bekanntgabe unterschiedliche Voraussetzungen.

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. Schriftliche Unterlagen zu Routineauskünften müssen nach Erledigung vernichtet werden. Sind Dokumente nach Ablauf der Aufbewahrungsfrist vernichtet worden, entfällt das Auskunftsrecht ganz.

Die Einwohnerkontrolle muss für die verschiedenen Arten der Datenbekanntgabe festlegen, welche Dokumente für wie lange aufbewahrt werden müssen. 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.

Sowohl der Verband Zürcher Einwohnerkontrollen (VZE) als auch der Verein Zürcher Gemeindeschreiber (VZGV) haben das Merkblatt positiv aufgenommen und ihren Mitgliedern zur Verfügung gestellt. Damit soll eine einheitliche Rechtspraxis der Einwohnerkontrollen im Kanton Zürich gewährleistet werden.

Titel: Wesensprüfung mit Hundehalterdaten
URL: http://www.datenschutz.ch/themen/1340.php
Datum: 26.08.2008

05.

Wesensprüfung mit Hundehalterdaten

Die Wesensprüfung eines Hundes entscheidet, ob ein Hund vom Leinen- und Maulkorbzwang befreit werden kann. Das Veterinäramt muss die Wesensprüfung dokumentieren. Bei der gefilmten Aufzeichnung darf auch der Hundehalter erfasst werden.

Für bestimmte Hunderassen gilt im öffentlichen Raum ein Leinen- und Maulkorbzwang. Das Veterinäramt kann Ausnahmen bewilligen, wenn die Wesensprüfung des Hundes eine solche Befreiung rechtfertigt.

Ein Hundehalter fragte den Datenschutzbeauftragten an, ob beim Wesenstest auch der Hundehalter gefilmt werden dürfe. Der Datenschutzbeauftragte bat darauf das Veterinäramt, ihm den Ablauf für eine Ausnahmebewilligung zu schildern und verschiedene Fragen zu beantworten.

Das Veterinäramt beurteilt das Wesen eines Hundes gestützt auf § 7a Hundeverordnung. Im Rahmen der Dokumentationspflicht der Amtsstellen wird die Wesensbeurteilung gefilmt. So muss zum Beispiel ein Gutachter auf entsprechende Aufzeichnungen zurückgreifen können. Eine Aufzeichnung ist auch nötig, damit dem Hundehalter der Entscheid erklärt werden kann oder zur Beweisführung im Rekursfall. Der gefilmte Wesenstest wird auf einer DVD in der Bewilligungsakte, die unter Verschluss steht, aufbewahrt. Zugriff haben ausschliesslich die zuständigen Sachbearbeitenden und Gutachter sowie im Einzelfall die Amtsleitung. Die Aufnahmen werden nicht auf einem Server gespeichert, und von der DVD werden keine Kopien erstellt.

Der Datenschutzbeauftragte gelangte zum Schluss, dass die Aufzeichnung der Wesensprüfung für eine Ausnahmebewilligung vom Leinen- und Maulkorbzwang verhältnismässig ist. Das Veterinäramt hatte zudem organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten getroffen. Nur die Aufbewahrung und die Löschung der DVD werden mit der Inkraftsetzung des neuen Hundegesetzes genauer zu regeln sein.

Titel: Einsicht in Personalakten
URL: http://www.datenschutz.ch/themen/1341.php
Datum: 26.08.2008

06.

Einsicht in Personalakten

Die Geschäftsprüfungskommission des Kantonsrates (GPK) kann Einsicht in Amtsakten nehmen, sofern die Akten für die Aufgabenerfüllung der GPK geeignet und erforderlich sind. Auch Personalakten können unter dieses Einsichtsrecht fallen.

Der Regierungsrat bat den Datenschutzbeauftragten abzuklären, ob die Geschäftsprüfungskommission des Kantonsrates (GPK) Einsicht in Kündigungsschreiben und Protokolle der Austrittsgespräche von Mitarbeitenden nehmen könne.

Die GPK ist für die Prüfung des Geschäftsberichts des Regierungsrates zuständig. Sie prüft und überwacht auch die Geschäfte der staatlichen Verwaltung, die der Regierungsrat beschlossen hat. Zudem prüft sie die ihr zugewiesenen Aufsichtseingaben über die kantonale Verwaltung sowie andere Spezialberichte. Die GPK erhält dazu ein Einsichtsrecht (§ 34e Kantonsratsgesetz). Dieses grundsätzliche Einsichtsrecht in die entsprechenden Amtsakten ist so weit gegeben, wie die Akten für die Aufgabenerfüllung der GPK geeignet und erforderlich sind. Unter Berücksichtigung des Verhältnismässigkeitsprinzips ist der GPK somit Einsicht in die verlangten Dossiers zu gewähren.

Im vorliegenden Fall betonte der Datenschutzbeauftragte, dass das Einsichtsrecht in die Kündigungsschreiben und in die Protokolle der Austrittsgespräche separat zu beurteilen sei.

Jede Datenbekanntgabe wird eingeschränkt, wenn überwiegende öffentliche oder private Interessen vorliegen (§ 10 DSG). Entsprechend weist auch das Kantonsratsgesetz darauf hin, dass anstelle der Herausgabe von Amtsakten ein besonderer Bericht erstattet werden kann, damit ein schutzwürdiges privates Interesse gewahrt, die Persönlichkeit geschützt oder ein hängiges Justizverfahren berücksichtigt werden kann (§ 34e Abs. 2 Kantonsratsgesetz).

Ob ein schutzwürdiges Interesse der austretenden Mitarbeitenden einer Herausgabe der Unterlagen an die GPK entgegensteht, ist in jedem Einzelfall separat zu beurteilen. Überwiegende schutzwürdige Interessen können beispielsweise vorliegen, wenn die Akten besonders schützenswerte Personendaten wie Informationen über die Gesundheit oder den persönlichen Geheimbereich enthalten.

Ein besonderer Bericht soll nur verfasst werden, wenn dies zur Wahrung der schutzwürdigen Interessen unerlässlich ist. Den schutzwürdigen Interessen betroffener Personen kann auch mit einer eingeschränkten Datenbekanntgabe begegnet werden (z.B. durch die Abdeckung bestimmter Stellen).

Titel: Patientendaten an das kantonale Krebsregister
URL: http://www.datenschutz.ch/themen/1342.php
Datum: 26.08.2008

07.

Patientendaten an das kantonale Krebsregister

Obwohl für das kantonale Krebsregister keine gesetzliche Grundlage besteht, können Spitäler im Kanton Zürich Patientendaten unter gewissen Einschränkungen an das kantonale Krebsregister weitergeben. Denn für Datenbearbeitungen zu nicht personenbezogenen Zwecken gelten erleichterte Voraussetzungen.

Der Datenschutzbeauftragte wurde von einem Zürcher Spital gebeten abzuklären, ob auch nicht anonymisierte Patientendaten dem kantonalen Krebsregister zur Verfügung gestellt werden dürften.

Obwohl Personendaten nur gestützt auf eine gesetzliche Grundlage bearbeitet werden dürfen, besteht für die Datenbeschaffung des kantonalen Krebsregisters lediglich ein Regierungsratsbeschluss von 1995. Ungeachtet dessen kann ein Spital im Kanton Zürich Personendaten an das kantonale Krebsregister weiterleiten, weil erleichterte Voraussetzungen für Datenbearbeitungen zu nicht personenbezogenen Zwecken gelten (§ 12 DSG). Das kantonale Krebsregister darf somit Personendaten für Forschung, Planung oder Statistik bearbeiten, wenn die Daten anonymisiert werden, sobald es der Bearbeitungszweck erlaubt und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. Diese Grundsätze gelten, wenn das verantwortliche Organ selbst «eigene» Personendaten zu nicht personenbezogenen Zwecken bearbeitet, aber auch wenn ein Dritter Daten eines öffentlichen Organs zu solchen Zwecken erhält.

Ein öffentliches Organ darf Personendaten unter folgenden Voraussetzungen an Dritte zur Bearbeitung zu nicht personenbezogenen Zwecken weitergeben: Die Bekanntgabe darf nicht durch eine Geheimhaltungspflicht oder eine andere Bestimmung ausgeschlossen werden und Rückschlüsse auf die betroffenen Personen müssen möglichst erschwert sein.

Wenn zum Beispiel im Rahmen eines Forschungsvorhabens nicht anonyme Personendaten an Dritte weitergegeben werden sollen oder wenn die Daten im Besitz einer Arztperson oder einer anderen an das Berufsgeheimnis gebundenen Person sind (Art. 321 bis StGB sowie Art. 32 DSG), müssen die verantwortlichen Forschenden zudem ein besonderes Verfahren einhalten: Sie müssen bei der Sachverständigenkommission ein Gesuch um Aufhebung des Berufsgeheimnisses einreichen. Ein solches Gesuch und die Bewilligung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung (Verfügung vom 27.2.1995) liegen für das kantonale Krebsregister vor – Letztere in Form einer Quellenbewilligung: Die Quellen, insbesondere die in der Schweiz praktizierenden Arzt- und Spitalarztpersonen, deren Hilfspersonen und Beauftragte (z.B. Laboratorien) sowie die Vereinigung Schweizerischer Krankenhäuser, werden ermächtigt, nicht anonymisierte Daten im Umfang des Bewilligungszwecks und in entsprechender Form an das kantonale Krebsregister weiterzuleiten.

Die öffentlichen Spitäler im Kanton Zürich können somit Daten an das kantonale Krebsregister weitergeben, sind allerdings nicht dazu verpflichtet.

Titel: Motionen zur Polizeidatenbank Polis
URL: http://www.datenschutz.ch/themen/1343.php
Datum: 26.08.2008

08.

Motionen zur Polizeidatenbank Polis

Zwei Motionen der Geschäftsprüfungskommission des Kantonsrates (GPK) befassen sich mit der Polis-Datenbank und verlangen Verbesserungen in Bezug auf diese sensiblen Datenbearbeitungen.

Die Kantonspolizei Zürich sowie die Stadtpolizeien von Zürich und Winterthur betreiben seit 1998 gemeinsam das Polizeiinformationssystem Polis. Die Datensammlung über Personen und Ereignisse dient der Polizei neben anderen Zwecken auch als Rechercheinstrument bei Ermittlungen und Lagebeurteilungen und enthält fast alle polizeilich relevanten Vorgänge. Rund 5000 Mitarbeitende der angeschlossenen Polizeien haben Zugriff auf Polis.

Damit die Polizei ihre Aufgaben erfüllen und eine Geschäftskontrolle führen kann, ist sie grundsätzlich befugt, Daten zu bearbeiten und dazu geeignete Datenbearbeitungssysteme zu betreiben. Zudem kann die Kantonspolizei den kommunalen Polizeien Zugriff auf ihre Datenbestände gewähren, soweit dies notwendig ist, damit diese Polizeien ihre Aufgaben erfüllen können.

Die Geschäftsprüfungskommission des Kantonsrates (GPK) befasste sich mit verschiedenen Aspekten der Polis-Datenbank und besprach sich auch mit dem Datenschutzbeauftragten.

Die auf der Grundlage der Polis-Verordnung gesammelten Personendaten sind besonders sensibel. Auch in Anbetracht der grossen Zahl von Personen (ca. 600 000), die im System verzeichnet sind, sind klare Rahmenbedingungen notwendig. Wegen ihrer weit gefächerten Aufgaben erfasst die Polizei im Polis die unterschiedlichsten Daten. Polis dient somit nicht nur der Ermittlung und Fahndung, sondern dokumentiert auch das polizeiliche Handeln. Die Daten entsprechen dem Erkenntnisstand zum Zeitpunkt der Eingabe und werden – vorbehältlich der Löschung – nicht von Amtes wegen nachgeführt. Der Grund, weshalb jemand im Polis gespeichert ist – beispielsweise als Zeuge oder Verdächtigter –, ist nicht auf den ersten Blick ersichtlich. Personen, welche erfahren, dass sie im Polis gespeichert sind, müssen allenfalls aktiv werden und eine Berichtigung ihrer Daten verlangen. Sie können dabei lediglich eine ergänzende Eintragung beantragen – ein Anspruch auf Löschung der Daten wird nicht akzeptiert. Personendaten, die im Zusammenhang mit einem Verfahren erhoben wurden, bleiben zum Teil sehr lange im System, auch wenn das Verfahren eingestellt wurde oder mit einem Freispruch endete. Begründet wird dies damit, dass Polis ein polizeiliches Arbeits- und Dokumentationsmittel sei und kein Strafregister.

Der Kantonsrat hat Ende April 2007 zwei Motionen der GPK an den Regierungsrat überwiesen. Motion 351/2006 fordert, dass Polis in ein operatives System und in ein Archivsystem aufgeteilt werden soll. Das operative System soll nur die aktuellen Fahndungsdaten umfassen und nach Abschluss der Ermittlungen oder des Verfahrens nur Daten über rechtskräftig verurteilte Personen speichern. Andere Personendaten sollen danach ins Archivsystem verschoben werden. Diese Aufteilung soll verhindern, dass Polis weiterhin Personen mitführt, gegen die nichts vorliegt. Motion 352/2006 verlangt, dass eine unabhängige Behörde – in diesem Fall der Datenschutzbeauftragte – die Nachführung oder Aktualisierung der Polis-Daten regelmässig kontrolliert.

Titel: Entsorgte Akten bleiben vertraulich
URL: http://www.datenschutz.ch/themen/1344.php
Datum: 26.08.2008

09.

Entsorgte Akten bleiben vertraulich

Um vertrauliche Akten zur Vernichtung zu sammeln, werden in Ämtern oft speziell gesicherte Sammelcontainer bereitgestellt. Wie bei einem Aktenschredder dürfen eingeworfene Akten nicht mehr herausgenommen werden können – auch nicht bei versehentlichem Einwurf.

Ein Amt liess vom Datenschutzbeauftragten das Entsorgungskonzept juristisch prüfen. Dieses sah vor, dass vertrauliche Akten in verschlossenen Containern gesammelt und von einer externen Firma vernichtet werden sollten. Angestellte, die Akten irrtümlicherweise in den Container werfen, sollen ein Gesuch zum Öffnen des Containers stellen können; das Gesuch müsste zusätzlich von einer vorgesetzten Amtsperson ab einer gewissen Funktionsstufe unterzeichnet werden.

Der Datenschutzbeauftragte beurteilte das Szenario zum Öffnen des Containers als nicht rechtmässig. Einerseits kann die Durchsuchung des Containers nach den irrtümlich entsorgten Akten zu einer Amtsgeheimnisverletzung führen, wenn dabei in Akten Einblick genommen wird, die im Schutzbereich von Art. 320 StGB liegen. Andererseits besteht das Risiko, dass Nichtberechtigte Einsicht in persönliche Unterlagen von Mitarbeitenden nehmen. Die Angestellten müssen sich darauf verlassen können, dass zur Vernichtung bestimmte Akten niemandem mehr zugänglich sind. Soll die Möglichkeit vorbehalten sein, einen Container im Notfall öffnen zu können, ist dies auf den Containern klar zu deklarieren.

Das Amt änderte daraufhin das Entsorgungskonzept und retournierte sämtliche Schlüssel dem externen Entsorgungsunternehmen. Werden Akten nun irrtümlich in einem solchen Container entsorgt, ist dies nicht mehr rückgängig zu machen. Funktional entsprechen die Container somit einem Aktenschredder.

Titel: Weltanschauung von Erwerbslosen
URL: http://www.datenschutz.ch/themen/1345.php
Datum: 26.08.2008

10.

Weltanschauung von Erwerbslosen

Ein Verein integriert im Auftrag eines Sozialamts Erwerbslose in eine Erwerbstätigkeit. Sein Bericht an das Sozialamt enthielt Aussagen über die Erwerbslosen, die keinen Bezug zum Arbeitsverhältnis hatten. Ein Arbeitnehmer, der damit nicht einverstanden ist, kann eine Berichtigung verlangen.

Ein Verein wurde von einem Sozialamt beauftragt, erwerbslose Personen in eine Erwerbstätigkeit zu integrieren. Eine betroffene Person beanstandete beim Datenschutzbeauftragten die Datenbearbeitungen dieses Vereins: Der Verein sammle über die Erwerbslosen auch Daten, die keinen Arbeitsplatzbezug aufwiesen, wie beispielsweise politische und gesellschaftliche Ansichten. Zudem habe der Verein das Sozialamt ohne Wissen der Klienten über diese Ansichten informiert.

Soweit der Verein öffentliche Aufgaben wahrnimmt oder mit öffentlichen Aufgaben von den Gemeinden beauftragt wird, gilt für die Datenbearbeitung das kantonale Datenschutzgesetz. Damit das Sozialamt die Tätigkeit des Vereins beaufsichtigen kann, darf der Verein die dazu geeigneten und notwendigen Informationen dem Sozialamt bekannt geben.

Ein Arbeitgeber darf Daten über die Arbeitnehmenden erheben, die für das Arbeitsverhältnis geeignet und erforderlich sind. Eine Erhebung von politischen und gesellschaftlichen Ansichten gehört nicht dazu. Die von der betroffenen Person beanstandeten Aussagen liessen jedoch nicht auf eine entsprechende Erhebung schliessen; vielmehr handelte es sich dabei um eine pauschale Wertung des Arbeitgebers.

Wer ein schützenswertes Interesse hat, kann vom verantwortlichen Organ verlangen, dass es die Folgen eines widerrechtlichen Bearbeitens beseitigt oder die Widerrechtlichkeit des Bearbeitens feststellt (§ 19 DSG). Es kann auch verlangt werden, dass das verantwortliche Organ Daten berichtigt oder vernichtet. Entspricht das Organ dem Begehren nach § 19 DSG nicht, erlässt es einen begründeten Entscheid (§ 20 Abs. 1 DSG). Dieser kann auf dem verwaltungsrechtlichen Weg angefochten werden.

In diesem Sinne riet der Datenschutzbeauftragte der betroffenen Person, sie solle verlangen, dass der Bericht des Vereins an das Sozialamt berichtigt werde.

Titel: Merkblatt für Sozialinspektoren
URL: http://www.datenschutz.ch/themen/1346.php
Datum: 26.08.2008

11.

Merkblatt für Sozialinspektoren

Wenn ein Verdacht auf Sozialhilfemissbrauch besteht, können Sozialämter Sozialinspektoren einsetzen. Zur Klärung der datenschutzrechtlichen Rahmenbedingungen bei solchen Einsätzen hat der Datenschutzbeauftragte ein Merkblatt verfasst.

Der Datenschutzbeauftragte erhielt verschiedene Anfragen zum Einsatz von Sozialinspektoren. Er wandte sich an das kantonale Sozialamt und bat um eine Stellungnahme aus fachlicher Sicht.

Sozialinspektoren werden von den Sozialämtern der Gemeinden eingesetzt, wenn ein Verdacht auf Sozialhilfemissbrauch besteht. Sie überprüfen, ob die Angaben der Personen, die Sozialhilfe beziehen, zutreffend sind. Diese Kontrollen können durch eigene Mitarbeitende oder durch beauftragte Drittpersonen erfolgen. Die Mittel, die für die Abklärungen eingesetzt werden, müssen verhältnismässig sein. Auch beauftragte Drittpersonen dürfen nur die Mittel anwenden, die das Sozialamt bei seinen Abklärungen einsetzen darf.

Damit die datenschutzrechtlichen Rahmenbedingungen bei einem Einsatz von Sozialinspektoren geklärt sind und einheitlich umgesetzt werden, hat der Datenschutzbeauftragte für die Sozialämter das Merkblatt «Einsatz von Sozialinspektoren im Kanton Zürich: Datenschutzrechtliche Rahmenbedingungen» verfasst. Es klärt vor allem folgende Punkte:

Bei Verdacht auf unrechtmässigen Sozialhilfebezug muss das Sozialamt den Sachverhalt abklären. Die gesuchstellende Person hat die Pflicht, dabei mitzuwirken. Sie ist mit einem Verdacht zu konfrontieren.

Wird ein sorgfältig ausgewählter und instruierter Sozialinspektor mit der Abklärung beauftragt, bleibt das Sozialamt für die Abklärung weiterhin verantwortlich. Der Auftrag ist zu präzisieren; dem Sozialinspektor dürfen nur die zur Auftragserfüllung notwendigen Informationen mitgeteilt werden.

Das Sozialamt hat mit schriftlicher Vereinbarung sicherzustellen, dass sich der Sozialinspektor an die datenschutzrechtlichen Vorgaben sowie an die Schweigepflicht hält. Informationen darf er nur für das Sozialamt, welches ihm den Auftrag erteilt hat, verwenden. Er hat die Informationen zudem sicher aufzubewahren und sie bei Vertragsauflösung dem Auftraggeber herauszugeben.

Für die Sachverhaltsabklärung dürfen die Informationen und Unterlagen beigezogen werden, die dafür geeignet und erforderlich sind. Es kommen wie für das Sozialamt selbst die Befragung Beteiligter oder von Auskunftspersonen, der Beizug von Amtsberichten, Urkunden und Sachverständigen oder ein Augenschein in Frage. Der Sozialinspektor hat keine weiterreichenden Befugnisse.

Die Informationen sind in erster Linie bei der gesuchstellenden Person zu beschaffen. Sie hat eine Mitwirkungspflicht. Werden weitere Auskünfte eingeholt, ist die gesuchstellende Person entsprechend zu informieren.

Titel: Einzel-, Listenauskünfte und Webpublikation
URL: http://www.datenschutz.ch/themen/1347.php
Datum: 26.08.2008

12.

Einzel-, Listenauskünfte und Webpublikation

Öffentliche Organe können Personendaten an Privatpersonen bekannt gegeben, wenn dafür gesetzliche Grundlagen bestehen. Für Auskünfte im Einzelfall, Listenauskünfte sowie für eine Publikation im Amtsblatt oder im Internet gelten unterschiedliche Regelungen.

Immer wieder stellen sich Fragen bei der Bekanntgabe von Personendaten durch öffentliche Organe. Der Datenschutzbeauftragte erarbeitete deshalb eine Zusammenstellung über die wichtigsten Punkte.

Damit ein öffentliches Organ beurteilen kann, ob es Personendaten an Privatpersonen bekannt geben darf, muss es alle entsprechenden Bestimmungen, welche auf verschiedene Erlasse auf eidgenössischer, kantonaler und kommunaler Ebene verteilt sein können, zusammentragen.

Einzelauskunft ohne Voraussetzung

Ein öffentliches Organ kann Einzelauskünfte in einigen Fällen voraussetzungslos an private Dritte erteilen; eine entsprechende Anfrage genügt. So erteilt die Einwohnerkontrolle Auskünfte über Name, Vorname, Adresse, Zu- und Wegzugsdatum sowie Beruf an private Dritte und das Steueramt stellt Ausweise über das steuerbare Einkommen und Vermögen aus.

Privatpersonen, die nicht wollen, dass die Einwohnerkontrolle oder das Steueramt Einzelauskünfte über sie an Dritte erteilen, können Datensperren errichten. Dasselbe gilt für das Verzeichnis der Fahrzeughalter beim Strassenverkehrsamt. Trotz Datensperre sind öffentliche Organe jedoch in bestimmten Fällen gesetzlich verpflichtet, Daten auch über diese Privatpersonen an Dritte bekannt zu geben, wenn eine gesuchstellende Person oder Organisation glaubhaft macht, dass die Datensperre einer Person sie in der Verfolgung eigener Rechte behindere.

Datenbanken, die via Internet nach vorgegebenen Kriterien Daten über Privatpersonen zugänglich machen, unterstehen strengeren Vorgaben: Weil es sich um ein Abrufverfahren handelt, müssen Einzelauskünfte dieser Art gesetzlich ausdrücklich vorgesehen sein. Technisch muss zudem sichergestellt sein, dass keine Serienanfragen möglich sind. Besondere Bestimmungen gelten für die öffentlichen Register des Privatrechtsverkehrs wie Handelsregister oder Grundbuch.

Einzelauskunft unter Voraussetzungen

In den meisten Fällen können Einzelauskünfte auf Anfrage privater Dritter nur unter bestimmten Voraussetzungen gewährt werden. Voraussetzungen sind beispielsweise der Nachweis oder die Glaubhaftmachung eines Interesses oder die persönliche Anwesenheit, beispielsweise bei einer Trauung. Einzelauskünfte können unter bestimmten Voraussetzungen auch aus dem Stimmregister, dem Natur- und Heimatschutzinventar, aus Gerichtsakten, aus Stellungnahmen in amtlichen Vernehmlassungsverfahren oder durch die Einwohnerkontrolle zu Geburtsdatum, Zivilstand und Heimatort einer Person erteilt werden.

Listenauskunft

Listenauskünfte können auf Anfrage privater Dritter nur gewährt werden, wenn sie als solche gesetzlich explizit zugelassen sind. Datensperren, die betroffene Personen errichtet haben, sind dabei aber zu beachten. Am häufigsten gibt die Einwohnerkontrolle Adressen in Listenform für schützenswerte ideelle Interessen an Private heraus.

Publikation im Internet

Die Veröffentlichung von Personendaten im Internet bedarf einer ausdrücklichen gesetzlichen Grundlage. Eine solche besteht beispielsweise für Amtsblätter.

Bei den meisten veröffentlichten Personendaten überwiegt nach einer gewissen Zeit das Interesse der betroffenen Personen, dass diese Daten gelöscht werden, oder das öffentliche Interesse an den Daten erlischt. Beides ist bei der Publikation zu berücksichtigen: Werden die Personendaten in einem Dokument mit anderen Inhalten angeboten – beispielsweise als PDF in Archiven von Printmedien, die auch amtliches Publikationsorgan sind –, muss sichergestellt sein, dass die ganzen Dokumente nicht mehr zugänglich sind, wenn sich die Personendaten anders nicht entfernen lassen. Dass amtliche Informationen mit Personendaten zeitlich beschränkt zugänglich sind, wird allerdings häufig unterlaufen, indem Private diese Informationen übernehmen und anbieten.

Die Zusammenstellung des Datenschutzbeauftragten hilft den öffentlichen Organen, zu beurteilen, unter welchen Voraussetzungen sie Privatpersonen Auskünfte über Dritte erteilen können. Bei einer Publikation von Personendaten im Internet muss das öffentliche Organ besonders beachten, dass es diese zwar in seinem eigenen Zugriffsbereich löschen kann, eine vollständige Entfernung aus dem Internet jedoch praktisch unmöglich ist.

Titel: Datenschutzgesetz und Aufsichtsbeschwerde
URL: http://www.datenschutz.ch/themen/1348.php
Datum: 26.08.2008

13.

Datenschutzgesetz und Aufsichtsbeschwerde

Obwohl das Datenschutzgesetz in Verfahren der Verwaltungsrechtspflege nicht anwendbar ist, gilt es bei der Behandlung von Aufsichtsbeschwerden. So auch im konkreten Fall, in dem im Rahmen einer Aufsichtsbeschwerde ein Bezirksrat von einem Amt Angaben über fehlbare Bauern einverlangte.

Weil ein Bauer gegen Direktzahlungsrichtlinien des Bundes verstossen hatte, wurde ihm der Pachtvertrag von einer Gemeinde nicht verlängert. Der Landwirt erhob beim Bezirksrat Aufsichtsbeschwerde mit der Begründung, der neu eingesetzte Pächter habe gegen die gleiche Richtlinie verstossen. Der Bezirksrat forderte darauf vom zuständigen kantonalen Amt verschiedene Angaben über Bauern der betroffenen Gemeinde, welche die Direktzahlungsrichtlinie nicht eingehalten hatten.

Das Amt wandte sich an den Datenschutzbeauftragten mit der Frage, ob es dem Bezirksrat Amtshilfe leisten und die verlangten Auskünfte erteilen müsse (§ 8 Abs. 1 lit. a DSG). Weil Verfahren der Verwaltungsrechtspflege nicht im Geltungsbereich des Datenschutzgesetzes liegen, musste der Datenschutzbeauftragte vorab seine Zuständigkeit in diesem Fall klären.

Die Aufsichtsbeschwerde ist gesetzlich nicht geregelt, lässt sich aber aus der Aufsichtsbefugnis der übergeordneten Verwaltungsbehörde über die hierarchisch untergeordnete herleiten. Weil die Aufsichtsbeschwerde kein förmliches Rechtsmittel, sondern ein blosser Rechtsbehelf ist, fällt sie nicht unter die Ausschlussklausel des Datenschutzgesetzes (§ 3 Abs. 2 lit. b DSG).

Der Datenschutzbeauftragte stellte seine Zuständigkeit fest und legte sodann dem Amt dar, auf welche Punkte es bei der Amtshilfe besonders achten müsse. Insbesondere darf Amtshilfe nur geleistet werden, wenn eine gesetzliche Aufgabe vom Empfänger nicht auf andere Weise erfüllt werden kann (Prinzip der Subsidiarität). Im Weiteren müssen die Daten für die Erfüllung der Aufgaben des Empfängers geeignet sein (Prinzip der Verhältnismässigkeit). Schliesslich ist das Prinzip der Zweckidentität zu beachten: Die um Amtshilfe ersuchende Verwaltungsstelle darf die Daten nur für einen Zweck gebrauchen, der mit dem ursprünglichen Verwendungszweck der Daten vereinbar ist. Es muss also eine gleichartige Aufgabe erfüllt werden.

Titel: Eignungsabklärung für bestimmte Berufe
URL: http://www.datenschutz.ch/themen/1349.php
Datum: 26.08.2008

14. Eignungsabklärung für bestimmte Berufe

Für eine Berufsausbildung in Pädagogik- oder Gesundheitsberufen wird abgeklärt, ob sich jemand dafür auch eignet. Daten, die im Rahmen von Eignungstests erhoben und weitergeleitet werden, müssen in jedem einzelnen Fall für den jeweiligen Abklärungszweck unentbehrlich sein.

Für Berufsausbildungen in Pädagogik- oder Gesundheitsberufen müssen gewisse Eignungsvoraussetzungen erfüllt werden. Dazu gehören eine entsprechende Vorbildung oder das Bestehen einer Zulassungsprüfung, in der die intellektuelle und praktische Eignung getestet wird. Aufgrund einer Anfrage einer betroffenen Person hat der Datenschutzbeauftragte sich mit der Frage auseinandergesetzt, welche Informationen hierzu geeignet und erforderlich sind.

Im Bereich der Pädagogik- und Gesundheitsberufe wird, gestützt auf einzelne Facherlasse, die persönliche Eignung vertieft abgeklärt. Um beispielsweise an die höhere Fachschule im Gesundheitswesen zugelassen zu werden, muss ein ärztliches Zeugnis beigelegt werden. Dieses ist durch den Vertrauensarzt der Schule zu prüfen. Bei einem Standortgespräch wird die soziale Eignung der Kandidierenden geprüft. Für die Ausbildung als Berufsfachschullehrer wird eine Eignungsbeurteilung verlangt, die aus einer persönlichen Standortbestimmung und einem Assessment besteht; bei Zweifeln an der Eignung kann eine erweiterte Eignungsbeurteilung angeordnet werden. Für die Zulassung zum Studium an der pädagogischen Hochschule wird die persönliche und gesundheitliche Eignung vorausgesetzt; bei Zweifeln kann ebenfalls eine erweiterte Eignungsabklärung durchgeführt werden. Dazu kann der Schularzt beigezogen oder die Begutachtung durch eine Fachperson angeordnet werden.

Bei der Abklärung der persönlichen Eignung werden überwiegend besonders schützenswerte Personendaten bearbeitet. Dies bedeutet, dass diese Daten von den Aufnahmewilligen in jedem einzelnen Fall nur dann erhoben oder weitergeleitet werden dürfen – beispielsweise an Mentorierende, Dozierende, Vertrauensarztpersonen oder Studienleitungen –, wenn sie für die konkreten Aufgaben der verschiedenen Beteiligten unentbehrlich sind. Nur so lange dürfen diese Daten auch aufbewahrt werden. Selbstverständlich sind auch die erhöhten Sicherheitsanforderungen bei der Bearbeitung besonders schützenswerter Personendaten zu beachten.

Der Datenschutzbeauftragte hat die betroffene Person beraten und festgestellt, dass zunehmend Eignungstests für Berufsbildungen durchgeführt werden. Die sich daraus ergebenden Fragestellungen werden aufmerksam zu verfolgen sein, damit nur die für den jeweiligen Abklärungszweck unentbehrlichen Daten bearbeitet werden.

Titel: Videoübertragung als Datenbearbeitung
URL: http://www.datenschutz.ch/themen/1350.php
Datum: 26.08.2008

15.

Videoübertragung als Datenbearbeitung

Eine Live-Übertragung mittels Videokameras auf Monitore fällt in den Geltungsbereich des Datenschutzgesetzes – auch wenn die übertragenen Daten nicht aufgezeichnet werden.

Eine städtische Verwaltungsbehörde wollte öffentliche Ausstellungsräume in einem Verwaltungsgebäude mit Videokameras überwachen. Weil eine Überwachung mit Personal als zu teuer befunden wurde, waren Direktübertragungen auf einen oder allenfalls mehrere Monitore vorgesehen. Auf eine Aufzeichnung der Bilder sollte allerdings verzichtet werden. Die Verwaltungsbehörde wandte sich an den kommunalen Datenschutzbeauftragten mit der Frage, ob die geplante Live-Übertragung ohne Speicherung der Bilder unter den Geltungsbereich des Datenschutzgesetzes falle.

Damit das Datenschutzgesetz einheitlich angewendet und ausgelegt wird, gelangte der kommunale Datenschutzbeauftragte mit dieser Frage an den Datenschutzbeauftragten.

In seiner Stellungnahme hält der Datenschutzbeauftragte fest, dass die geplante Videoübertragung tatsächlich unter das Datenschutzgesetz falle. Er begründet dies damit, dass beim geplanten Vorhaben Daten durch eine Kamera erhoben, übermittelt und auf einem Monitor bekannt gegeben werden. Auch ohne Aufzeichnung der übertragenen Daten liegt deshalb eine Datenbearbeitung im Sinne von § 2 lit. f DSG vor.

Titel: Meldepflicht für ausländische Sozialhilfebezüger
URL: http://www.datenschutz.ch/themen/1351.php
Datum: 26.08.2008

16.

Meldepflicht für ausländische Sozialhilfebezüger

Das neue Ausländergesetz führt die Meldepflicht für sozialhilfeabhängige Ausländerinnen und Ausländer ein. Gemeinden, die Sozialhilfe zahlen, müssen das Migrationsamt über Beginn, Umfang und Beendigung eines Sozialhilfebezugs informieren.

Gemäss dem neuen Ausländergesetz (AuG), das per 1.1.2008 in Kraft getreten ist, kann die Aufenthaltsbewilligung widerrufen werden, wenn eine Ausländerin oder ein Ausländer auf Sozialhilfe angewiesen ist (Art. 62 lit. b AuG). Auch eine Niederlassungsbewilligung kann widerrufen werden, wenn eine Ausländerin oder ein Ausländer dauerhaft und in erheblichem Mass auf Sozialhilfe angewiesen ist (Art. 63 Abs. 1 lit. c AuG).

Das Migrationsamt gelangte an den Datenschutzbeauftragten mit der Frage, welche Informationen die neu eingeführte Meldepflicht für sozialhilfeabhängige Ausländerinnen und Ausländer umfasse.

Der Bundesrat bestimmt, welche Daten den Ausländerbehörden beim Bezug von Sozialhilfe zu melden sind (Art. 97 Abs. 3 lit. d AuG). Die Behörden, die für die Ausrichtung der Sozialhilfe zuständig sind – im Kanton Zürich die Gemeinden –, melden der zuständigen kantonalen Ausländerbehörde den Bezug von Sozialhilfe (Art. 82 Abs. 5 der Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit, VZAE). Der Bundesrat führte diese Angaben nicht näher aus.

Der Datenschutzbeauftragte kam zu folgendem Schluss: Das Migrationsamt muss bei sozialhilfeabhängigen Ausländerinnen und Ausländern einen allfälligen Widerruf der Aufenthalts- oder der Niederlassungsbewilligung prüfen. Dazu sind die Angaben über Beginn, Umfang und Beendigung des Sozialhilfebezugs geeignet und notwendig. Gestützt auf die Meldepflicht (Art. 82 Abs. 5 VZAE) müssen die Gemeinden diese Informationen dem Migrationsamt bekannt geben.

Titel: Kostengutsprache braucht keine Diagnose
URL: http://www.datenschutz.ch/themen/1352.php
Datum: 26.08.2008

17.

Kostengutsprache braucht keine Diagnose

Für eine Kostengutsprache nach einer unvorhergesehenen Spitalbehandlung darf das Sozialamt nur nach den Gesundheitsdaten fragen, die für die Anspruchsabklärung geeignet und erforderlich sind. Anstelle einer medizinischen Diagnose reicht dazu eine Umschreibung der Behandlungsursache.

Spitäler können bei den zuständigen Sozialämtern Kostengutsprachen für unvorhergesehene Behandlungskosten einholen, die sie weder beim Patienten noch anderweitig geltend machen können. Sie müssen dazu ein Formular des Sozialamts des Kantons Zürich verwenden. Dieses Formular sah vor, dass die Spitäler über ihre Patientinnen und Patienten auch sensible Daten wie die medizinische Diagnose angeben.

Arzt- und ihre Hilfspersonen unterstehen dem strafrechtlich geschützten Berufsgeheimnis nach Art. 321 StGB. Ausnahmen sind nur legitim, wenn eine ausreichende gesetzliche Grundlage vorhanden ist. Diese muss präzisieren, wer wem welche Daten bekannt geben muss oder darf. Die Sozialhilfeverordnung sieht bei einem Notfall eine medizinische Behandlung ohne vorgängige Kostengutsprache vor. Soll ein Sozialamt solche unvorhergesehenen Behandlungskosten übernehmen, muss das Gesuch des Spitals folgende zusätzlichen Angaben enthalten (§§ 20 und 21 SHV): allfällige Garanten, Angaben zur Notwendigkeit, Art, Umfang und Dauer der Leistungen und Anlass für die Behandlung. Die medizinische Diagnose wird nicht verlangt. Das Sozialamt überprüft anschliessend, ob tatsächlich nur benötigte sowie wirtschaftliche Behandlungen durchgeführt wurden. Dazu ist jedoch keine medizinische Diagnose erforderlich; es genügt, wenn eine Arztperson die Behandlungsursache kurz umschreibt.

Die Angabe der Diagnose ist deshalb aus dem Gesuchsformular zu streichen. Es genügt, dass die Behandlungsursache kurz umschrieben wird. Der Datenschutzbeauftragte forderte das Sozialamt auf, das Formular anzupassen, was entsprechend erledigt wurde.

Titel: Skilager mit Folgen für die Schulpflege
URL: http://www.datenschutz.ch/themen/1353.php
Datum: 26.08.2008

18. Skilager mit Folgen für die Schulpflege

Die Schulpflege einer Primarschule führte ein Skilager durch. Während des Lagers kam es zu teilweise strafrechtlich relevanten Vorfällen ohne Nachweis der Täterschaft. Die Bekanntgabe der Namen der Verdächtigen an alle Eltern und die Sekundarstufe war weder gesetzes- noch verhältnismässig.

Die Lagerleitung informierte auf Anweisung der Schulpflege sowohl die Eltern der Lagerteilnehmenden als auch die Sekundarstufe über verschiedene Delikte und Disziplinarvergehen, die sich während eines Skilagers der Mittelstufe ereignet hatten. Das Schreiben enthielt eine Namensliste der mutmasslich beteiligten Schüler.

Die Eltern eines Schülers, der auf der Namensliste aufgeführt war, wandten sich an die Schulpflege und beschwerten sich über die Weiterleitung der Namen an Schulpflege und Sekundarstufe; der Stufenübertritt stand noch bevor.

Der Datenschutzbeauftragte beurteilte auf Anfrage dieser Eltern das Vorgehen der Schulpflege als nicht rechtmässig: Es lagen weder eine gesetzliche Grundlage noch eine Einwilligung der Betroffenen vor, welche die Schulpflege berechtigt hätte, der Oberstufe die Namen der mutmasslich fehlbaren Schüler mitzuteilen. Da zudem nicht ausgewiesen war, zu welchen konkreten Beanstandungen der betroffene Schüler Anlass gegeben hatte, war die Benachrichtigung unverhältnismässig. Auf blossen Verdächtigungen beruhende Informationen sind weder geeignet noch erforderlich, den Ablauf eines künftigen Skilagers positiv zu beeinflussen.

Aufgrund der Einschätzung des Datenschutzbeauftragten forderten die Eltern von der Schulpflege die Löschung der Personendaten ihres Sohnes – was die Schulpflege jedoch nicht tat.

Die Eltern wandten sich schliesslich mit dem ausserordentlichen Rechtsmittel der Aufsichtsbeschwerde an die Direktion der Justiz und des Innern, welche den Datenschutzbeauftragten in seiner Einschätzung stützte. Sie wies die Schulpflege an, die Namensliste der Lagerleitung in den Akten der Sekundarstufe zu vernichten.

Titel: Fachgutachter im Beschwerdeverfahren
URL: http://www.datenschutz.ch/themen/1354.php
Datum: 26.08.2008

19.

Fachgutachter im Beschwerdeverfahren

Im Beschwerdeverfahren sind Beschwerdeinstanzen grundsätzlich an die Feststellungen des Datenschutzbeauftragten gebunden.

Der Datenschutzbeauftragte hat den Auftrag, die Anwendung der Vorschriften über den Datenschutz durch öffentliche Organe zu überwachen (§ 23 i.V.m. § 1 DSG). Die Direktion der Justiz und des Innern konkretisierte die Bedeutung von Stellungnahmen des Datenschutzbeauftragten für eine verfügende Behörde in einem Beschwerdeverfahren.

Die Feststellungen des Datenschutzbeauftragten haben den Stellenwert eines Fachgutachtens. Nicht von Bedeutung ist, ob der Datenschutzbeauftragte im konkreten Fall von der betroffenen Person oder von dem zuständigen öffentlichen Organ um eine Beurteilung der Sachlage angefragt wird.

Der entscheidenden Behörde steht die freie Würdigung des Sachverhaltes grundsätzlich zu. Sie ist jedoch an die Feststellungen des Datenschutzbeauftragten gebunden, sofern sie keine triftigen Gründe für eine abweichende Haltung vorbringen kann. Die Gebundenheit erschliesst sich bereits aus der koordinationsrechtlichen Überlegung, dass Stellungnahmen kantonaler Fachstellen in hinreichendem Ausmass zu berücksichtigen sind. Gemäss einem Entscheid des kantonalen Verwaltungsgerichtes gilt dies auch für andere sachkundige (Spezial)behörden, deren Berichte wegen der besonderen Fachkompetenz eigentlichen Gutachten gleichkommen, denen bei der Entscheidfindung grosses Gewicht zukommt. Als triftige Gründe für eine abweichende Haltung gelten insbesondere Irrtümer, Lücken oder Widersprüche, die ein Gutachten enthalten könnte.

Kantonale Behörden sind daher nicht befugt, ihre Auslegung datenschutzrechtlicher Fragen anstelle derjenigen einer unabhängigen Fachstelle zu setzen. Dies gilt verstärkt für Fragen des Datenschutzes auf kommunaler Ebene, weil dafür in der Regel keine separate Behörde oder Stelle zuständig ist. Zudem besteht stets das Risiko, dass die spezifischen Sachinteressen durch die entscheidende Behörde gegenüber den Interessen der Querschnittsaufgabe Datenschutz stärker gewichtet werden.

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. Beatrice Glaser
lic. iur. Karin Brunner Steib
lic. iur., RA Raphael Weiss

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

Beratungsstelle für Informatiksicherheit (BIS)
vakant

Kommunikation
Dr. phil. Andrea Ruf

Sekretariat
Martina Richard
Susanne Brüngger

Tätigkeitsbericht Nr. 13 (2007)
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