Tätigkeitsbericht

2009

ab 1.10.2008

dsb
datenschutzbeauftragter
kanton zürich

Tätigkeitsbericht 2009

Der Datenschutzbeauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht (§ 39 Gesetz über die Information und den Datenschutz [IDG]).

Der Tätigkeitsbericht 2009 deckt den Zeitraum vom 1. Oktober 2008 (Inkrafttreten des IDG) bis 31. Dezember 2009 ab.

Zürich, März 2010

Der Datenschutzbeauftragte des Kantons Zürich

Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Klare Regeln für neue Technologien

Neue Informationstechnologien durchdringen zunehmend alle Lebensbereiche und sind mit wachsenden Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger verbunden. Ob Smart Meters, Websites oder Videoüberwachung: Zum Schutz der Privatheit müssen Datenbearbeitungen klar geregelt sein. **6**

Aufwändige Einführung des IDG

Die Einführung des Öffentlichkeitsprinzips und die zunehmende Bearbeitung sensitiver Daten bilden grosse Herausforderungen für den Schutz der Grundrechte der Bürgerinnen und Bürger. **8**

Publikationen 2009

abrufbar unter www.datenschutz.ch/publikationen

Leitfäden
- Datenschutz im Sozialbereich
- Videoüberwachung

Merkblätter
- Personendaten für Forschungsvorhaben
- Vorabkontrolle

Einsatz von Parkplatzdetektiven

Gemeinden sind gestützt auf die Strassenverkehrsgesetzgebung befugt, eine eigene Verordnung für das regelmässige nächtliche Abstellen von Fahrzeugen zu erlassen. Für die Nutzung des öffentlichen Grundes dürfen Gebühren erhoben und betroffene Fahrzeughalter können einer Meldepflicht unterstellt werden. Gemeinden dürfen Dritte mit den dazu notwendigen Überwachungsaufgaben beauftragen. **37**

Harmonisierung der Einwohnerregister

Die Umsetzung des Registerharmonisierungsgesetzes muss gewährleisten, dass Daten, die zu statistischen Zwecken erhoben werden, nicht anderweitig verwendet werden. Auch die Ersterfassung der Grunddaten durch eine Drittfirma muss ausschliessen, dass diese Firma die Daten zu eigenen Zwecken nutzen kann. Eine künftige Verwendung der Sozialversicherungsnummer in den Registern braucht eine bereichsspezifische Regelung. **46**

Vollmacht für Vertrauensarzt

Pensionskassen entscheiden aufgrund einer vertrauensärztlichen Untersuchung über die Leistung bei Berufs- und Erwerbsinvalidität. Versicherte sind grundsätzlich zu einer vertrauensärztlichen Untersuchung verpflichtet. Die Vollmacht, mit der sie den Vertrauensarzt ermächtigen, Auskünfte einzuholen, muss hinreichend bestimmt sein: Versicherte müssen aus dieser erkennen können, zu welchem Zweck der Vertrauensarzt welche Auskünfte über sie bei Dritten einholt und der Pensionskasse weitergibt. **51**

VII. Ausgewählte Fälle

Klare Regeln für neue Technologien

Neue Informationstechnologien durchdringen zunehmend alle Lebensbereiche und sind mit wachsenden Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger verbunden. Ob Smart Meters, Websites oder Videoüberwachung: Zum Schutz der Privatheit müssen Datenbearbeitungen klar geregelt sein.

Intelligente Stromzähler, sogenannte Smart Meters, sollen den Stromverbrauch von Privathaushalten viertelstündlich messen und Daten automatisiert an die Stromlieferanten weiterleiten. Ein Pilotprojekt sieht vor, dass mit diesen Messdaten die monatliche Rechnungsstellung an die Privathaushalte erfolgt. Um die gesamte Energieeffizienz zu erhöhen, sollen auch die Stromlastspitzen der Haushalte präzis bestimmt werden.

Die Energienutzung in Privathaushalten widerspiegelt Tagesabläufe. Wird der Stromverbrauch viertelstündlich gemessen und punktgenau abgelesen, lässt sich auf die Gewohnheiten der Bewohnerinnen und Bewohner schliessen. Elektronische Stromverbrauchsdaten einer Person sind deshalb Personendaten. Sie lassen sich mit anderen Daten dieser Person verknüpfen, wodurch Persönlichkeitsprofile erstellt werden können. Deshalb sind die Grundsätze des Datenschutzes strikte zu beachten und die Verwendung der Daten klar zu regeln.

Der Datenschutzbeauftragte beriet die Elektrizitätswerke des Kantons Zürich (EKZ), wie sie diese datenschutzrechtlichen Grundsätze für einen flächendeckenden Einsatz von Smart Meters sicherstellen können: Die Messintervalle können sowohl für die monatliche Rechnungsstellung als auch für den Gesamtenergieverbrauch verlängert werden. Zudem muss der Zweck mindestens in einer Verordnung festgehalten werden. Der Datenschutzbeauftragte prüfte das Pilotprojekt Smart Meters im Rahmen einer Vorabkontrolle (siehe Seite 30).

Neue Vorabkontrolle

Die Vorabkontrolle wurde mit dem Gesetz über die Information und den Datenschutz (IDG), das per 1. Oktober 2008 in Kraft getreten ist, eingeführt: Öffentliche Organe müssen geplante Datenbearbeitungen dem Datenschutzbeauftragten vorlegen, wenn das Projekt besondere Risiken für die Rechte und Freiheiten der betroffenen Personen enthält, damit diese Risiken frühzeitig erkannt und vermieden werden können.

Der Datenschutzbeauftragte führte bereits verschiedene Vorabkontrollen durch. Sowohl im rechtlichen als auch im organisatorischen und technischen Bereich konnte er so rechtzeitig die konkreten Anforderungen im Bereich des Datenschutzes aufzeigen, wodurch aufwändigere Nachbesserungen bei der technischen Umsetzung vermieden werden konnten. Anhand eines Merkblatts können öffentliche Organe einfach klären, ob sie eine geplante Datenbearbeitung zur Vorabkontrolle melden müssen (www.datenschutz.ch/publikationen). Der Datenschutzbeauftragte prüft jede Anfrage individuell und erteilt eine formalisierte Stellungnahme. Seine Prüfung kann auch ergeben, dass auf eine formelle Vorabkontrolle verzichtet wird (siehe Seite 12).

Vorgaben für Internetnutzung

Der Datenschutzbeauftragte berät immer häufiger öffentliche Organe, die das Internet in ihre Verwaltungsabläufe integrieren.

Für ihre Websites nutzen öffentliche Organe zunehmend Dienstleistungen von Dritten, wie dynamische Karten oder Statistikauswertungen. Nutzende, die diese Dienste auf einer Website anwählen, geben ihre IP-Adresse nicht nur dem öffentlichen Organ als Betreiber der Website an, sondern auch dem Anbieter des jeweiligen Dienstes. Ein öffentliches Organ darf solche Dienste Dritter grundsätzlich in seine Website integrieren. Weil es jedoch auch für die Datenbearbeitung des Drittangebotes verantwortlich bleibt, muss es einen schriftlichen Vertrag mit dem Dritten abschliessen und Links auf Drittangebote klar als solche kennzeichnen (siehe Seite 15).

Berichte über die Qualität der Schulen in pädagogischer und organisatorischer Hinsicht können auf dem Internet veröffent-

licht werden, soweit sie keine Informationen enthalten, die einer bestimmbaren Person zugeordnet werden können. Dies kann durch Anonymisierung erreicht werden oder indem die Rahmenbedingungen einer Funktion beurteilt werden – und nicht die Person, die diese Funktion wahrnimmt (siehe Seite 31).

Geschäfte von Gemeindeversammlungen, die Personendaten enthalten, dürfen publiziert werden, wenn die Personendaten für die stimmberechtigten Gemeindemitglieder geeignet und erforderlich sind. Eine Bekanntgabe an einen weiteren Adressatenkreis – insbesondere über das Internet – erfordert eine hinreichend bestimmte Rechtsgrundlage, welche die Internetpublikation ausdrücklich vorsieht (siehe Seite 35).

Es finden sich aber auch Websites, die indirekt mit öffentlichen Organen verbunden sind. So werden zunehmend Websites angeboten, die eine Bewertung von Lehrkräften oder Dozierenden sowie deren Lehrveranstaltungen ermöglichen. Anhand von anonym eingegebenen Bewertungen erstellen sie eine Art «Zeugnis» für die jeweiligen Lehrpersonen. Solche Bewertungen sind weder verlässlich noch aussagekräftig. Sie eignen sich deshalb nicht, die Qualität der Lehre an (Hoch-) Schulen zu verbessern. Bewertungen, die ohne Einwilligung der betroffenen Lehrkraft erfolgen, sind grundsätzlich nicht gerechtfertigt. Die (Hoch-)Schule hat als Arbeitgeberin gegenüber den angestellten Lehrkräften eine Fürsorgepflicht und muss bei den Betreibern intervenieren, wenn die Website persönlichkeitsverletzende Einträge enthält. Lehrpersonen können ausserdem mit einer Zivilklage oder Strafanzeige gegen die Websitebetreiber vorgehen (siehe Seite 14).

Videoüberwachung transparent regeln

Nicht nur die Zahl der Anfragen zum Thema Videoüberwachung nimmt beim Datenschutzbeauftragten zu. Auch die geplanten Einsatzorte werden immer unterschiedlicher: So prüfen nun auch öffentliche Organe wie Jagdaufseher oder Spitäler den Einsatz von Videokameras. Der beabsichtigte Zweck bleibt indessen immer derselbe: Die Videoüberwachung soll Vandalismus vermeiden oder zur Sicherheit beitragen.

Mit der Videoüberwachung werden hauptsächlich Personendaten bearbeitet. Die öffentlichen Organe dürfen solche Daten bearbeiten, soweit dies für ihre gesetzlichen Aufgaben geeignet und erforderlich ist. Es genügt, wenn die entsprechende Aufgabe des öffentlichen Organs in einer rechtlichen Grundlage umschrieben ist und sich die Videoüberwachung als Mittel zur Erfüllung dieser Aufgabe ableiten lässt.

Aus Gründen der Transparenz empfiehlt der Datenschutzbeauftragte den öffentlichen Organen, in jedem Fall ein Reglement zur Videoüberwachung zu erlassen. Eine Hilfestellung dazu bieten der neue Leitfaden des Datenschutzbeauftragten «Videoüberwachung durch öffentliche Organe» (www.datenschutz.ch/publikationen) sowie das Musterreglement (siehe Seite 13).

Klare Regeln

Neue Informationstechnologien brauchen klare Regeln, um den Schutz der Privatheit der Bürgerinnen und Bürger zu gewährleisten. Das Instrument der Vorabkontrolle stellt sicher, dass datenschutzrechtliche Anliegen rechtzeitig berücksichtigt werden. Beim praktischen Einsatz schaffen konkrete Regelungen die notwendige Transparenz. Damit kann auch in einer zunehmend technisierten Gesellschaft das Grundrecht auf persönliche Freiheit respektiert werden.

Aufwändige Einführung des IDG

Die Einführung des Öffentlichkeitsprinzips und die zunehmende Bearbeitung sensitiver Daten bilden grosse Herausforderungen für den Schutz der Grundrechte der Bürgerinnen und Bürger.

Am 1. Oktober 2008 ist das Informations- und Datenschutzgesetz (IDG) in Kraft getreten und hat das Datenschutzgesetz (DSG) abgelöst. Der gesetzgeberische Schritt vom DSG zum IDG ist keine reine Formalität: Das IDG bringt einschneidende materielle Änderungen für die öffentlichen Organe, die im Wesentlichen vier Bereiche betreffen:

- die gesetzliche Umsetzung des durch die Verfassung garantierten Öffentlichkeitsprinzips;
- die Anpassungen des Datenschutzrechts an die europarechtlichen Vorgaben;
- die Schnittstelle zwischen Informationszugang und Datenschutz;
- die vollständige Unabhängigkeit des Datenschutzbeauftragten.

Die Berichterstattungsperiode war geprägt von der Umsetzung der neuen Bestimmungen in der Praxis. Diese Umsetzung erwies sich aufwändiger als erwartet.

Systemwechsel Öffentlichkeitsprinzip

Der Systemwechsel vom Geheimhaltungsprinzip zum Öffentlichkeitsprinzip erforderte nicht nur eine Anpassung der Informationspolitik, sondern auch der Prozesse der einzelnen Verwaltungsstellen. Dabei gibt das IDG Rahmenbedingungen, die von der Verordnung über die Information und den Datenschutz (IDV) in diesem Bereich konkretisiert werden. Die einzelnen öffentlichen Organe haben diese Aufgaben unterschiedlich gelöst. Während auf kantonaler Ebene die Koordinationsstelle IDG bei der Staatskanzlei die Direktionen bei der Umsetzung des Öffentlichkeitsprinzips unterstützt, fehlt für die übrigen öffentlichen Stellen und insbesondere für die Gemeinden eine solche Instanz. Im Gegensatz zum Bund und zu den übrigen Kantonen, die das Öffentlichkeitsprinzip neu eingeführt haben, verzichtete der Gesetzgeber im Kanton Zürich, dem Datenschutzbeauftragten auch die Funktion des Informationszugangs- oder Öffentlichkeitsbeauftragten zu übertragen. Damit fehlt einerseits eine kantonsweite Stelle, welche die öffentlichen Organe im Bereich des Informationszugangs berät; bei den einzelnen Stellen fällt dadurch Mehraufwand an, wie sich nun bereits in der Einführungsphase zeigt. Andererseits ist mittel- und längerfristig zu befürchten, dass sich keine einheitliche Praxis in Bezug auf den Informationszugang entwickelt und damit Einzelfälle nur in aufwändigen Gerichtsverfahren geklärt werden können.

Da sich beim Informationszugang gemäss dem Öffentlichkeitsprinzip häufig datenschutzrechtliche Fragen stellen – wenn die Bekanntgabe von Informationen auch Personendaten umfasst –, ist der Datenschutzbeauftragte gleichwohl oft in entsprechende Beratungen involviert. Dabei bleibt unbefriedigend, dass sich aufgrund der unterschiedlichen Zuständigkeiten mehrere Stellen mit der gleichen Frage befassen müssen.

Anpassungen des Datenschutzrechts

Die Anpassungen des Datenschutzrechts an die europarechtlichen Vorgaben haben zu zwei wichtigen institutionellen Neuerungen geführt, die im Vorfeld der Datenbearbeitungen und bei der nachträglichen Kontrolle zu einer Stärkung der Rechte der Bürgerinnen und Bürger beitragen.

Im Rahmen der Vorabkontrolle haben die öffentlichen Organe beabsichtigte Datenbearbeitungen, die besondere Risiken für die Rechte und Freiheiten der betroffenen Personen enthalten können, dem Datenschutzbeauftragten zur Prüfung vorzulegen. Solche Risiken liegen insbesondere vor, wenn umfangreiche Datenbearbeitungen geplant sind oder besondere technische Verfahren eingesetzt werden sollen. Bereits in den ersten

Monaten nach Inkraftsetzung des IDG sind verschiedene Projekte zur Vorabkontrolle eingereicht worden (siehe Seite 12). Die Prüfung durch den Datenschutzbeauftragten erstreckt sich dabei auf die rechtlichen, organisatorischen und technischen Aspekte der jeweiligen Datenbearbeitungen. Einige der vorgelegten Projekte wurden nicht als Vorabkontrolle qualifiziert, und im Rahmen einer Beratung wurden dem zuständigen Organ entsprechende Hinweise gegeben. Wichtig bei der Vorabkontrolle ist, dass die Prüfung bereits in einem frühen Projektstadium durchgeführt werden kann, damit notwendige Rechtsanpassungen oder organisatorische und technische Anpassungen noch rechtzeitig vor Inbetriebnahme vorgenommen werden können. Obwohl zahlreiche Projekte dem Datenschutzbeauftragten vorgelegt wurden, kann nicht davon ausgegangen werden, dass sämtliche relevanten Projekte mittels Vorabkontrollen erfasst sind. Um den öffentlichen Organen diesbezüglich eine Hilfestellung zu geben, hat ihnen der Datenschutzbeauftragte das Merkblatt «Vorabkontrolle» mit einer Checkliste zur Verfügung gestellt. Der Datenschutzbeauftragte hat die Vorabkontrollen innert angemessener Frist vorzunehmen; da sich die Prüfungen als komplex und aufwändig erweisen, hat dies angesichts einer angespannten Ressourcensituation bereits in der Einführungsphase zu einigen Verzögerungen geführt.

Als neues Instrument des Datenschutzes steht nun auch eine gerichtliche Beurteilung von Empfehlungen des Datenschutzbeauftragten zur Verfügung: Stellt der Datenschutzbeauftragte bei seinen Tätigkeiten Verletzungen von Bestimmungen über den Datenschutz fest, kann er dem öffentlichen Organ Empfehlungen geben, welche Massnahmen zu ergreifen sind. Falls ein Organ eine solche Empfehlung nicht umsetzen will, hat es eine Verfügung zu erlassen. Diese Verfügung kann vom Datenschutzbeauftragten angefochten werden. Seit Inkrafttreten des IDG hat der Datenschutzbeauftragte noch keine förmlichen Empfehlungen erlassen. Vielmehr wurden den öffentlichen Organen im Rahmen der Beratungs- und der Kontrolltätigkeit Hinweise gegeben, wie sie den Datenschutz angemessen umzusetzen haben. Soweit diese Hinweise befolgt werden, liegt kein Grund für eine weiter gehende Empfehlung vor. Somit ist es noch zu keinen Verfügungen seitens öffentlicher Organe gekommen, die eine vorgeschlagene Massnahme des Datenschutzbeauftragten ablehnen. Die weitere Praxis wird zeigen, wie weit das Instrument der gerichtlichen Überprüfung von Empfehlungen präventiv wirkt, so dass Datenschutzanliegen bereits von Anfang an angemessen berücksichtigt werden.

Schnittstelle Informationszugang

Wie erwartet zeigte sich die Schnittstelle zwischen Informationszugang und Datenschutz in der Praxis als der Bereich, der bei der Umsetzung des IDG am meisten Fragen aufwirft. Der Datenschutzbeauftragte war in den ersten Monaten nach Inkraftsetzung des IDG mit einem hohen Anstieg der Beratungen von öffentlichen Organen und Privatpersonen konfrontiert, der über die gesamte Berichtsperiode anhielt. Sowohl bei der Informationstätigkeit von Amtes wegen als auch bei der Bekanntgabe von Informationen auf individuelles Gesuch hin sind häufig Personendaten betroffen. Das IDG regelt diese Schnittstelle klar: Die Informationstätigkeit von Amtes wegen enthält nur Personendaten, soweit es sich um die Ansprechpersonen eines öffentlichen Organs handelt oder die gesetzlichen Voraussetzungen für eine Bekanntgabe von Personendaten vorliegen. Sofern bei einem Informationsgesuch einer Bürgerin oder eines Bürgers auch Personendaten betroffen sind, hat eine Interessenabwägung stattzufinden. Dies ist auch der Fall, wenn eine Person im Rahmen des Auskunftsrechts Zugang zu den eigenen Personendaten will und Personendaten Dritter betroffen sind. Die Interessenabwägungen können nur im konkreten Einzelfall

vorgenommen werden. Aufgrund der noch fehlenden Praxis zum IDG haben die öffentlichen Organe noch grosse Mühe mit den formellen und materiellen Anforderungen in diesem Bereich und sind auf Unterstützung angewiesen. Es bleibt offen, wie sich der Aufwand für die öffentlichen Organe in diesem Bereich entwickeln wird. Dieser wird nicht nur von der Art und Weise, wie die Informationstätigkeit von Amtes wegen wahrgenommen wird, sondern auch von der Anzahl der individuellen Informationsgesuche abhängen. Wesentlich wird zudem eine umfassende Dokumentation der Praxis sein.

Vollständige Unabhängigkeit

Zu den Hauptanliegen der europarechtlichen Vorgaben gehört auch die Schaffung einer unabhängigen Stelle, die sich für die Anliegen des Datenschutzes und die Rechte der Bürgerinnen und Bürger einsetzt. Mit dem IDG wurden die Voraussetzungen für diese Vorgaben geschaffen: Das IDG gewährt die institutionelle Unabhängigkeit des Datenschutzbeauftragten. Die diesbezüglichen Bestimmungen wurden bereits vor der allgemeinen Inkraftsetzung des IDG umgesetzt, so dass der Zusatzaufwand beim Datenschutzbeauftragten gestaffelt angefallen ist. Einerseits mussten die administrativen Abläufe angepasst und andererseits die materiellen Anforderungen des IDG umgesetzt werden. Beides verursachte einen beträchtlichen Zusatzaufwand. Die institutionelle Unabhängigkeit warf in der Praxis Fragen in Bezug auf die Aufgaben und Kompetenzen der involvierten Stellen auf. Diese Fragen konnten aufgrund eines Gutachtens schrittweise angegangen werden. Die europarechtlichen Anforderungen verlangen zudem eine verstärkte Kontrolltätigkeit, die ebenfalls in der Berichtsperiode in die Wege geleitet werden konnte. Mit den übrigen Beratungs- und Vermittlungsaufgaben, den Informations- und Ausbildungstätigkeiten, die zum Pflichtenheft des Datenschutzbeauftragten gehören, sind die bestehenden Ressourcen mehr als ausgeschöpft. In der Praxis kann dieser Situation nur mit einer rigorosen Priorisierung begegnet werden, was indessen sowohl für die betroffenen öffentlichen Organe als auch für die Bürgerinnen und Bürger unbefriedigend ist. Die Unabhängigkeit des Datenschutzbeauftragten kann nur zur Stärkung der Rechte der Bürgerinnen und Bürger beitragen, wenn die Ressourcen in einem angemessenen Rahmen sind. Angesichts der wachsenden Datenbearbeitungen der öffentlichen Organe sind auch dem Datenschutzbeauftragten Ressourcen in einem verhältnismässigen Umfang zur Verfügung zu stellen. Speziell die Kontrolltätigkeit muss gestärkt werden.

Breites Tätigkeitsfeld

Der vorliegende Bericht bietet einen Überblick über die Schwerpunkte der Tätigkeiten und präsentiert ausgewählte Fälle. Er veranschaulicht, dass einerseits die Problemstellungen komplexer werden, und dass andererseits immer mehr Bereiche von sensitiven Datenbearbeitungen betroffen sind. Zahlreiche Angelegenheiten konnten zwar einer angemessenen Lösung zugeführt werden. Doch der Schutz der Rechte der Bürgerinnen und Bürger angesichts der Zunahme der Datenbearbeitungen in allen Bereichen bleibt eine Herausforderung: Eine bürgerorientierte Verwaltungstätigkeit muss auch einen effektiven Datenschutz gewährleisten.

Mit seinen Tätigkeiten unterstützt der Datenschutzbeauftragte die öffentlichen Organe bei der Umsetzung des Datenschutzes. Dabei ist es nicht immer selbstverständlich, dass die Interessen der Bürgerinnen und Bürger am Schutz ihrer Privatsphäre bei den Vorhaben der Verwaltung von Anfang an mitberücksichtigt werden. Die immensen Datenbearbeitungen entwickeln häufig eine Eigendynamik, und die datenschutzrechtlichen – aber vielfach auch die sicherheitstechnischen Anliegen – geraten in den Hintergrund. Mit einer rechtzeitigen

Beratung, aber auch mit nachträglichen Kontrollen schafft der Datenschutzbeauftragte den Anliegen des Datenschutzes Nachachtung. Im Gegensatz zu den finanziellen und personellen Mitteln, die jährlich für die Datenbearbeitungen der Verwaltung ausgegeben werden, stehen dem Datenschutzbeauftragten indessen keine verhältnismässigen Ressourcen zur Verfügung. Das Budget des Datenschutzbeauftragten beträgt weniger als ein Prozent der jährlichen Ausgaben der kantonalen Verwaltung für Informatik.

Dabei ist der Schutz der Privatheit in der Informations- und Kommunikationsgesellschaft zu einer generellen Herausforderung geworden. Der Staat spielt dabei eine besondere Rolle, wenn es um seine eigenen Datenbearbeitungen geht: Diese haben die persönliche Freiheit und die Privatsphäre der Bürgerinnen und Bürger zu respektieren. Hierfür braucht es für alle Datenbearbeitungen angemessene Rechtsgrundlagen. Der Staat hat aber auch im Rahmen der öffentlichen Bildung die Aufgabe, die Schülerinnen und Schüler, die Bürgerinnen und Bürger zu befähigen, ihre Grundrechte wahrzunehmen. Dazu gehört ein kompetenter Umgang mit den neuen Medien der Informations- und Kommunikationsgesellschaft. Beide Zielsetzungen sind Teil der Tätigkeiten des Datenschutzbeauftragten. In unserer liberalen Rechts- und Gesellschaftsordnung ist es unabdingbar, dass der Datenschutz tatsächlich gewährleistet ist und die Bürgerinnen und Bürger ihre Datenschutzrechte wahrnehmen können.

Der vorliegende Tätigkeitsbericht lädt auch dazu ein, sich der Rolle der Privatsphäre in Staat und Gesellschaft bewusster zu werden. Wie die Schwerpunktthemen und die einzelnen Fälle zeigen, gibt es kaum mehr einen Lebensbereich, der nicht von Datenbearbeitungen durchdrungen ist. Dabei wird auch immer deutlicher, wie wichtig der Schutz der Privatsphäre wird.

Gefragte Vorabkontrollen

Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen müssen dem Datenschutzbeauftragten zur Vorabkontrolle unterbreitet werden. In Einzelfällen kann er von einer formellen Vorabkontrolle absehen.

Öffentliche Organe müssen Datenbearbeitungen dem Datenschutzbeauftragten vorab zur Prüfung vorlegen, wenn das geplante Projekt besondere Risiken für die Rechte und Freiheiten der betroffenen Personen enthält. Mit dieser Neuerung durch das IDG können Risiken für die Persönlichkeitsrechte frühzeitig erkannt und vermieden werden. Im Unterschied zu den kontinuierlichen Kontrollen des Datenschutzbeauftragten wird im Rahmen der Vorabkontrolle eine Datenbearbeitung individuell und abgestimmt auf die jeweiligen Anforderungen geprüft. Geprüft werden vor allem die rechtlichen, aber auch die organisatorischen und technischen Rahmenbedingungen. Wenn solche Projekte frühzeitig und standardisiert auf die datenschutzrechtlichen Voraussetzungen geprüft werden, kann der finanzielle und zeitliche Aufwand, vor allem was die Ausgestaltung technischer Systeme betrifft, minimiert werden.

Damit die öffentlichen Organe einfach klären können, ob sie eine geplante Datenbearbeitung zur Vorabkontrolle melden müssen, erarbeitete der Datenschutzbeauftragte das Merkblatt «Vorabkontrolle» mit einer kurzen Checkliste (www.datenschutz.ch/publikationen).

Der Datenschutzbeauftragte führte in der Berichtsperiode verschiedene Vorabkontrollen durch, so zum Beispiel bei folgenden Projekten: Protokollierung der Daten der Benutzer- und Administrationsaktivitäten von IT-Systemen, Online-Zugriffe auf Datenbanken anderer Direktionen oder der Einsatz neuer Technologien wie Smart Meters (siehe auch Seite 30). Im Rahmen dieser Vorabkontrollen konnten sowohl im rechtlichen als auch im organisatorischen und technischen Bereich rechtzeitig Verbesserungen für den Datenschutz aufgezeigt werden. So wurde beispielsweise darauf hingewiesen, dass eine formell gesetzliche Grundlage für die Einführung eines Abrufverfahrens (Online-Zugriff) erforderlich sei, und es konnte auf weitere Massnahmen zur Informationssicherheit hingewiesen werden.

Bei weiteren Fällen verzichtete der Datenschutzbeauftragte auf eine formelle Vorabkontrolle und somit auf eine ausführliche Stellungnahme zu den rechtlichen, organisatorischen und technischen Rahmenbedingungen der Datenbearbeitung. Dabei handelte es sich jeweils um Projekte, für die Daten der Gebäudeversicherung benötigt wurden. So wurden für eine Strassenlärmsanierung zahlreiche Adressdaten der betroffenen Hauseigentümer und für eine Ortsplanungsrevision die Daten aller versicherten Gebäude benötigt. Zwar waren in diesen Fällen jeweils eine grosse Anzahl von Personen betroffen, womit ein Kriterium für eine Vorabkontrolle erfüllt war (§ 10 IDG i.V.m. § 24 IDV). Weil der Datenschutzbeauftragte jedoch den Eingriff in die Persönlichkeitsrechte der Betroffenen als gering erachtete, war eine formelle Vorabkontrolle nicht angezeigt. Die Datenbekanntgabe konnte auf das Gesetz über die Gebäudeversicherung abgestützt werden (§ 9a Abs. 2).

Die individuelle Prüfung einer geplanten Datenbearbeitung kann somit durchaus ergeben, dass auf eine formelle Vorabkontrolle verzichtet wird. Der Datenschutzbeauftragte prüft jede Anfrage individuell und erteilt eine formalisierte Stellungnahme.

Ausweitung der Videoüberwachung

Videokameras werden in immer unterschiedlicheren Bereichen eingesetzt. Jede Videoüberwachung durch öffentliche Organe muss sich auf eine rechtliche Grundlage stützen können und verhältnismässig sein. Ein Reglement schafft die erforderliche Transparenz.

Nicht nur die Zahl der Anfragen zum Thema Videoüberwachung nimmt beim Datenschutzbeauftragten zu; auch die geplanten Einsatzorte werden immer unterschiedlicher. Während bisher vor allem Schulen und Kirchen auf Videoüberwachung setzten (siehe auch Tätigkeitsbericht Nr. 14 [1.–9.2008], S. 25 f.), prüfen nun auch öffentliche Organe wie Jagdaufseher oder Spitäler den Einsatz von Videokameras. Doch ob für Jagdhochsitze oder die Patientenaufnahme im Spital, der beabsichtigte Zweck bleibt stets derselbe: Die Videoüberwachung soll Vandalismus vermeiden und zur Sicherheit der jeweiligen Institution sowie deren Angestellten und der die Institution Benutzenden beitragen. Auch die Anfragen an den Datenschutzbeauftragten enthalten stets die gleichen Unsicherheiten: Zum einen erkundigen sich die öffentlichen Organe nach den Anforderungen an die gesetzliche Grundlage und nach den einzuhaltenden datenschutzrechtlichen Rahmenbedingungen für eine Videoüberwachung. Zum anderen ist den öffentlichen Organen unklar, ob sie ein Reglement zu erlassen haben und wie sie konkret mit den Videoaufnahmen umgehen sollen.

Mit der Videoüberwachung werden hauptsächlich Personendaten bearbeitet. Die öffentlichen Organe dürfen solche Daten bearbeiten, soweit dies für ihre gesetzlichen Aufgaben geeignet und erforderlich ist. Es genügt, wenn die entsprechende Aufgabe des öffentlichen Organs in einer rechtlichen Grundlage umschrieben ist und sich die Videoüberwachung als Mittel zur Erfüllung dieser Aufgabe ableiten lässt.

Von einer Videoüberwachung können auch besondere Personendaten betroffen sein. Dies ist immer der Fall, wenn die Videoüberwachung durch Polizeiorgane vorgenommen wird. Oder wenn bei den aufgezeichneten Informationen aufgrund ihrer Bedeutung oder der Art der Bearbeitung die besondere Gefahr einer Persönlichkeitsverletzung besteht. Besondere Personendaten weisen aufgrund ihrer Sensibilität einen erhöhten Schutzbedarf auf; deren Bearbeitung bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz. Die Videoüberwachung selbst muss im Gesetz vorgesehen sein.

Auch wenn für eine Videoüberwachung eine ausreichende rechtliche Grundlage besteht, muss sie in jedem Fall verhältnismässig sein. Konkret hat das öffentliche Organ zu prüfen, ob der anvisierte Zweck nicht mit anderen Massnahmen erreicht werden könnte, die weniger in die Privatheit der Betroffenen eingreifen. Bleibt die Videoüberwachung das einzige geeignete Mittel, muss sie so ausgestaltet werden, dass sie die Privatheit der Betroffenen so wenig wie möglich tangiert und auch als solche gekennzeichnet ist.

Aus Gründen der Transparenz empfiehlt der Datenschutzbeauftragte den öffentlichen Organen, ein Reglement zur Videoüberwachung zu erlassen. Eine Hilfestellung dazu bieten der neue Leitfaden des Datenschutzbeauftragten «Videoüberwachung durch öffentliche Organe» (www.datenschutz.ch/publikationen) sowie das Musterreglement.

Websites zur Bewertung von Lehrkräften

Websites zur Bewertung von Lehrkräften und deren Veranstaltungen sind überwiegend unrechtmässig. Die (Hoch-)Schule hat bei den betreffenden Websitebetreibern zu intervenieren. Lehrpersonen können mit einer Zivilklage oder Strafanzeige gegen die Websitebetreiber vorgehen.

Zunehmend werden Websites angeboten, die eine Bewertung von Lehrerinnen, Dozenten und Professorinnen sowie deren Lehrveranstaltungen ermöglichen. Die Bewertungen können zumeist anonym und per Knopfdruck als Noten zum Unterricht oder zu der Person des Lehrers, der Dozentin oder des Professors eingegeben werden. Die Website errechnet darauf die Gesamtnote und dokumentiert sie als eine Art «Zeugnis». Häufig können auch Kommentare zur Lehrkraft oder zur Veranstaltung abgegeben werden. Mit Suchbegriffen wie Name und Vorname einer Lehrkraft können solche Einträge per Suchmaschine gefunden werden.

Die Bewertungen auf solchen Websites unterscheiden sich damit wesentlich vom Austausch unter Studierenden oder einer Bewertung mittels Fragebogen. Denn die Einträge auf diesen Websites sind praktisch unbeschränkt abruf- und kopierbar. Auch kann sich, wer will, auf solchen Websites als «Studierender» oder «Schülerin» registrieren lassen. Mit verschiedenen Benutzernamen kann ein Benutzer zudem eine Lehrperson oder -veranstaltung mehrfach bewerten.

Die Bewertungen auf solchen Online-Plattformen sind somit weder verlässlich noch aussagekräftig. Sie eignen sich deshalb nicht, die Qualität der Lehre an (Hoch-)Schulen zu verbessern. Im Vergleich zu herkömmlichen Bewertungsmethoden sind die Persönlichkeitsrechte einer Lehrperson zudem in erhöhtem Masse gefährdet. Bewertungen, welche ohne Einwilligung der betroffenen Lehrkraft erfolgen, sind grundsätzlich nicht gerechtfertigt. Das auf diese Weise wahrgenommene Recht auf Meinungsfreiheit mag das Recht der Lehrkraft auf informationelle Selbstbestimmung in den meisten Fällen nicht zu überwiegen.

Die (Hoch-)Schule hat als Arbeitgeberin gegenüber den angestellten Lehrkräften eine Fürsorgepflicht. Lehrkräfte, die dem Personalgesetz des Kantons Zürich unterstehen, haben Anspruch auf Schutz ihrer Persönlichkeit. Der Staat ist gesetzlich verpflichtet, die zum Schutz der persönlichen Integrität seiner Angestellten erforderlichen Massnahmen zu treffen (§ 39 Abs. 1 und 2 Personalgesetz). Es liegt deshalb an der (Hoch-)Schule, bei den betreffenden Websitebetreibern zu beantragen, dass persönlichkeitsverletzende Einträge beseitigt werden. Weiter kann die (Hoch-)Schule im Rahmen einer Disziplinarordnung Disziplinarmassnahmen androhen, wenn Sittlichkeit, Anstand und die gebührende Achtung gegenüber den Mitgliedern des Lehrkörpers verletzt werden (z.B. Verweis oder Ausschluss eines fehlbaren Schülers). Die (Hoch-)Schule kann die Bewertungen auf Online-Plattformen zudem einzudämmen versuchen, indem sie offizielle (hoch-)schulinterne Evaluationen durchführt.

Schliesslich besteht für betroffene Lehrkräfte die Möglichkeit, mit einer Zivilklage gegen die Websitebetreiber vorzugehen oder eine Strafanzeige gegen diese zu erstatten, sollte eine Bewertung in zivilrechtlicher Hinsicht eine widerrechtliche Verletzung der Persönlichkeit darstellen oder den Tatbestand eines Ehrverletzungsdelikts erfüllen.

Der Datenschutzbeauftragte hat anfragende (Hoch-)Schulen entsprechend beraten.

Dienste von Dritten auf Websites

Öffentliche Organe integrieren zunehmend Dienste von Dritten in ihre Websites. Sie bleiben für diese Angebote verantwortlich und müssen mit den Dritten schriftliche Verträge schliessen. Blosse Links auf fremde Angebote sind klar als solche zu kennzeichnen.

Von Wettervorhersagen über dynamische Karten bis zu Zugriffsstatistiken: Dritte bieten im Internet kostenlos oder gegen Gebühr unzählige Dienste an, die in Websites integriert werden können. Nutzende, die diese Dienste auf einer Website anwählen, geben ihre IP-Adresse nicht nur dem Betreiber der Website an, sondern auch dem Anbieter des jeweiligen Dienstes.

Gemäss einem Entscheid des Bundesverwaltungsgerichts (A-3144/2008 vom 27. Mai 2009) ist die IP-Adresse ein Personendatum, weil es eine eindeutige Identifizierung eines Rechners zulässt. Mittels IP-Adresse ist somit auch die Person bestimmbar, die eine Website aufgerufen hat. Meistens erhält der Anbieter eines Internetdienstes zusätzlich zur IP-Adresse Angaben zum verwendeten Browser und Betriebssystem sowie weitere Informationen, die sich anhand der IP-Adresse einer bestimmten Person zuordnen lassen.

Ein öffentliches Organ darf solche Dienste Dritter grundsätzlich in seine Website integrieren. Es bleibt jedoch auch für den integrierten Teil und die damit verbundene Datenbearbeitung verantwortlich.

Da die IP-Adressen der Nutzenden an Dritte übertragen werden, muss das öffentliche Organ die entsprechenden Vorschriften («Outsourcing») beachten. Das öffentliche Organ muss einen schriftlichen Vertrag mit dem Dritten abschliessen, der insbesondere Folgendes regelt: Gegenstand und Umfang der übertragenen Aufgaben, Umgang mit Personendaten, Geheimhaltungsverpflichtungen, Behandlung von Informationszugangsgesuchen, erforderliche Massnahmen zum Schutz der Information, Kontrolle der Auftragserfüllung, vorgesehene Sanktionen bei Vertragsverletzung sowie Vertragsdauer und die Voraussetzungen der Vertragsauflösung. Verwendet der Dritte die Personendaten nicht vertragsgemäss, droht ihm eine Busse. Zusätzliche Rahmenbedingungen gelten, wenn ein öffentliches Organ die Dienste von einem im Ausland domizilierten Anbieter oder Server bezieht.

Weil die Übertragung der Datenbearbeitung an Dritte gesetzlich zulässig ist, sofern die genannten Bedingungen eingehalten werden, müssen und können Benutzende der Website nicht einwilligen. Das öffentliche Organ muss jedoch Transparenz schaffen über die Angebote Dritter auf der eigenen Website und über die damit verbundenen Datenbearbeitungen.

Will ein öffentliches Organ auf ein nicht in seinen Aufgabenkreis gehörendes und nicht unter seiner Verantwortung stehendes Angebot eines Dritten, beispielsweise auf eine lokale Wettervorhersage, hinweisen, hat es auf seiner Website einen entsprechenden Link zu setzen und diesen aussagekräftig zu beschriften (z.B. «Wetter, zur Verfügung gestellt von xy»). Aus einem Link mit der blossen Bezeichnung «Wetter» darf geschlossen werden, es handle sich um ein Angebot der Gemeinde, für welches diese die Verantwortung trage.

Keine Datenbearbeitung im Auftrag findet statt, wenn das öffentliche Organ mit Zustimmung des Dritten die Applikation auch auf seinem eigenen Webserver betreibt und dem Dritten keine Informationen übermittelt.

Rechtliche Grundlagen für Online-Zugriffe

Ein Online-Zugriff auf Personendaten stellt einen erheblichen Eingriff in die Grundrechte der betroffenen Personen dar. Er ist nur zulässig, wenn ein Gesetz dies ausdrücklich vorsieht.

Mit einem Online-Zugriff können bestimmte Angaben aus einem Informationsbestand abgerufen werden. So können Untersuchungsbehörden beispielsweise online in Einwohnerregistern bestimmte Personendaten abfragen. Und anhand einer Kontrollschildnummer kann jedermann Name und Adresse des Fahrzeughalters auf der Website des Strassenverkehrsamtes abrufen.

Ein Online-Zugriff auf Personendaten stellt einen erheblichen Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. Der Abrufberechtigte kann auf Personendaten zugreifen, ohne dass die bekannt gebende Behörde jeweils davon Kenntnis hat. Die Behörde kann somit nicht beurteilen, ob die bezogenen Personendaten tatsächlich für die jeweilige Amtsaufgabe erforderlich waren. Das Risiko nimmt noch zu, wenn nicht nur Behörden, sondern auch Private online auf Personendaten zugreifen können. Hier kann nicht kontrolliert werden, zu welchem Zweck die bezogenen Personendaten verwendet werden.

Ein Online-Zugriff auf Personendaten ist nur zulässig, wenn er in einem Erlass ausdrücklich vorgesehen ist. Besondere Personendaten dürfen nur dann online zugänglich gemacht werden, wenn dies in einem hinreichend bestimmten formellen Gesetz geregelt ist. Der Online-Zugriff muss nicht nur ausdrücklich im Gesetz erwähnt sein; zusätzlich müssen insbesondere die Kategorien der Personendaten und der Verwendungszweck umschrieben sein. Es muss zudem im Gesetz festgelegt werden, wer die Personendaten abrufen kann – Behörden oder beliebige Personen – und ob nur Einzelabfragen oder auch Massenoperationen zulässig sind.

Gesetzesformulierungen, wonach Personendaten «öffentlich zugänglich» gemacht oder «zur Verfügung gestellt» werden können, sind nicht hinreichend bestimmt und bilden keine genügende Grundlage für den Online-Zugriff auf Personendaten. Behörden, die einen Online-Zugriff auf bestimmte Personendaten einrichten möchten, müssen dieses Vorhaben vorab dem Datenschutzbeauftragten zur Prüfung unterbreiten. Anzumerken ist, dass es technisch schwierig ist, Abfragen über Internet zahlenmässig zu beschränken; die gängigen Methoden zum Ausschluss von Massenoperationen wie Captchas, Cookies oder die Beschränkung von IP-Adressen können umgangen werden.

Das Öffentlichkeitsprinzip hat keinen Einfluss auf die Rechtsetzungsstufe und den Bestimmtheitsgrad einer rechtlichen Grundlage für einen Online-Zugriff. Es erleichtert zwar den Zugang zu amtlichen Informationen, jedoch nicht zu Personendaten Privater – weder mit noch ohne Online-Zugriff.

Klarer Rahmen für E-Government

Im Bereich E-Government befasste sich der Datenschutzbeauftragte mit den rechtlichen Grundlagen sowie der neuen Plattform «ZHservices». Zudem steckte er den Rahmen ab, in welchem elektronische Wahlen ohne Vorverfahren versuchsweise zulässig sind.

Die Stabsstelle E-Government erteilte Ende 2007 einen Auftrag für eine einheitliche, auf einem zentralen Personenstamm basierende Basisinfrastruktur (ServicePortal, heute «ZHservices»), mit der Privatpersonen und Unternehmen mit Verwaltungsstellen und diese untereinander Daten austauschen können. Der Datenschutzbeauftragte stellte fest, dass für den Betrieb einer solchen Plattform eine formellgesetzliche Grundlage geschaffen werden müsse. Da sich ähnliche Fragestellungen auch bei anderen E-Government-Projekten stellen, beauftragte der Regierungsrat eine Arbeitsgruppe, um den Regelungsbedarf für E-Government abzuklären. Die Arbeitsgruppe kam zum Schluss, dass keine übergeordnete Gesetzgebung für den Bereich E-Government geschaffen werden solle. Die gesetzlichen Regelungen seien im Rahmen der jeweiligen fachspezifischen E-Government-Projekte zu schaffen.

«ZHservices» wurde Mitte 2009 für Dienstverschiebungs- und Auslandurlaubsgesuche von Armee- und Zivilschutzangehörigen in Betrieb genommen. Der Datenschutzbeauftragte widersetzte sich dem nicht, stellte aber klar, dass für eine Ausweitung des Betriebes mit zentralisierter Datenbearbeitung gesetzliche Grundlagen geschaffen werden müssten. Er wies zudem darauf hin, dass das Amt für Militär und Zivilschutz sein Vorgehen mit den bestehenden Regelungen in Einklang zu bringen habe. Ob trotz Verzicht auf eine anerkannte Signatur Authentizität und Nachvollziehbarkeit in rechtlich genügendem Mass gewährleistet seien, werde in einem konkreten Anwendungsfall zu beurteilen sein. Aufgrund der Unterlagen konnte der Datenschutzbeauftragte nicht prüfen, ob die Vertraulichkeit ausreichend gewährleistet ist. Er erarbeitete deshalb zusammen mit der Stabsstelle E-Government einen Prüfungsauftrag; das Ergebnis ist noch ausstehend.

Bei Wahlen ohne Vorverfahren können Wahlberechtigte jeder wählbaren Person ihre Stimme geben. Bei der elektronischen Umsetzung, welche bisher einmal versuchsweise getestet wurde, können sie dafür die entsprechende Person im Stimmregister suchen und sie bezeichnen. Es kann allerdings nicht ausgeschlossen werden, dass der Zugriff auf das Stimmregister nicht nur zu Wahlzwecken verwendet wird. Der Datenschutzbeauftragte hat sich mit dem Statistischen Amt darauf verständigt, dass aufgrund der bestehenden Rechtslage die beiden Städte Zürich und Winterthur bei elektronischen Wahlen ohne Vorverfahren nicht in die laufenden Versuche einbezogen werden und diese auf kommunale Wahlen in den elf bereits beteiligten Gemeinden beschränkt bleiben. Zudem erhalten die Stimmberechtigten möglichst wenige Angaben zu wählbaren Personen, und Massenoperationen werden möglichst verhindert. Für eine Ausweitung der Versuche oder für die definitive Einführung der elektronischen Stimmabgabe ist eine Änderung des Gesetzes über die Politischen Rechte erforderlich.

Teilrevision des Sozialhilfegesetzes

Regelungen zur Bearbeitung von Informationen über Sozialhilfemassnahmen müssen hinreichend bestimmt sein. Für die betroffenen Personen muss ersichtlich sein, welche ihrer Personendaten von welcher Behörde zu welchem Zweck bearbeitet werden.

Der Datenschutzbeauftragte wurde eingeladen, sich im Rahmen des Vernehmlassungsverfahrens zum Entwurf für eine Teilrevision des kantonalen Sozialhilfegesetzes zu äussern. Insbesondere soll der Informationsaustausch zwischen den verschiedenen Behörden und Ämtern des Kantons und der Gemeinden im Bereich der Sozialhilfe geregelt werden. So sollen die Sozialhilfeorgane die Möglichkeit erhalten, bei anderen Behörden und Ämtern Auskünfte einzuholen, die sie für die Erfüllung ihrer gesetzlichen Aufgaben benötigen. Andererseits werden Sozialhilfeorgane gegenüber diesen Stellen zur Auskunft verpflichtet, sofern jene die Auskünfte ihrerseits für ihre Aufgabenerfüllung benötigen. Weiter soll der Sozialhilfemissbrauch erschwert werden: Kantonale und kommunale Behörden und Ämter sowie Organisationen und Personen mit öffentlichen Aufgaben sollen ermächtigt werden, bei einem Verdacht auf unrechtmässig erwirkte Sozialhilfeleistungen Mitteilung an die zuständigen Sozialhilfeorgane zu machen. Auch sollen nötigenfalls private Dritte gegenüber Sozialhilfeorganen zur Auskunft verpflichtet werden können.

In seiner Stellungnahme hielt der Datenschutzbeauftragte fest, dass Informationen über Sozialhilfemassnahmen besondere Personendaten sind, deren Bearbeitung einer hinreichend bestimmten formellgesetzlichen Regelung bedarf. Die betroffenen Personen müssen anhand des Gesetzes nachvollziehen können, welche ihrer Personendaten von welcher Behörde zu welchem Zweck bearbeitet werden dürfen. Gemäss den weiterhin geltenden Bestimmungen des Sozialhilfegesetzes und der zugehörigen Verordnung sollen die Angaben, die notwendig sind, um die finanziellen und persönlichen Verhältnisse abzuklären, nach wie vor in erster Linie beim Hilfesuchenden beschafft werden. Dieser ist verpflichtet – unter Hinweis auf die Straffolgen –, über seine Verhältnisse wahrheitsgemäss Auskunft zu geben und Einsicht in seine Unterlagen zu gewähren. Die Fürsorgebehörde darf nur Auskünfte bei Dritten einholen, wenn die Angaben des Hilfesuchenden angezweifelt werden oder wenn dieser seiner Mitwirkungspflicht nicht nachkommt. Zudem dürfen beim Hilfesuchenden oder bei Dritten nur die Auskünfte eingeholt werden, die für die Erfüllung der gesetzlichen Aufgaben der Sozialhilfeorgane geeignet und erforderlich sind. Dass auch Privatpersonen zur Auskunft gegenüber Sozialhilfeorganen verpflichtet werden sollen, ist insofern fragwürdig, als die damit beabsichtigte Wirkung in einem angemessenen Verhältnis zum Eingriff in die Grundrechte der betroffenen Personen stehen muss.

Die Anmerkungen des Datenschutzbeauftragten sind in den überarbeiteten Vernehmlassungsentwurf weitgehend eingeflossen. Der überarbeitete Entwurf ist wesentlich differenzierter formuliert, was sowohl den Betroffenen als auch den beteiligten Behörden und Ämtern mehr Transparenz und Rechtssicherheit bringt, ohne Letztere in ihrer Arbeit zu behindern oder die Aufdeckung von Missbräuchen zu erschweren. Zudem wird beispielsweise die Fürsorgebehörde erst dann zur Einholung von Auskünften bei Dritten ermächtigt, wenn Zweifel an der Richtigkeit oder Vollständigkeit der Angaben oder Unterlagen des Hilfesuchenden bestehen. Der Regierungsrat hat die Vorlage am 18. September 2009 zuhanden des Kantonsrates verabschiedet.

Geoinformationen und Datenlogistik

Seit mehreren Jahren fordert der Datenschutzbeauftragte gesetzliche Regelungen zu Geoinformationen und zur Datenlogistik. Der Entwurf des kantonalen Geoinformationsgesetzes berücksichtigt zwar wichtige Forderungen. Eine gesetzliche Grundlage für die Datenlogistik fehlt weiterhin.

Bereits 1996 befasste sich der Datenschutzbeauftragte mit Geoinformationen (siehe Tätigkeitsbericht Nr. 2 [1996]). Er stellte fest, dass es sich bei Gebäudedaten um Personendaten handle, sobald diese ausreichten, um ein Gebäude mittels Adresse oder Katasternummer zu individualisieren. Er forderte die Schaffung von Rechtsgrundlagen für das damals projektierte kantonale Geografische Informationssystem (GIS). Mit dessen Inbetriebnahme erliess der Regierungsrat 1998 die GIS-Verordnung. Drei Jahre später stellte er fest, dass ein kantonales Gesetz für die Einrichtung leistungsfähiger Informationssysteme und für die Verwendung grösserer Datenbestände öffentlicher Organe zu schaffen sei. In den Folgejahren wurde die Infrastruktur zur Datenverarbeitung in den Abteilungen GIS-Zentrum und Datenlogistik des Amtes für Raumordnung und Vermessung ohne genügende Rechtsgrundlagen weiter ausgebaut.

Mit dem Erlass des Bundesgesetzes über Geoinformation (GeoIG) Ende 2007 wurden die Kantone verpflichtet, eigene gesetzliche Regelungen für Geoinformationen zu schaffen. Der Regierungsrat beauftragte die Baudirektion Anfang 2008 mit der Ausarbeitung eines Entwurfes. Gleichzeitig trennte er die Gesetzgebung der Bereiche Datenlogistik und Geoinformationen. Er beauftragte die Baudirektion, die Gesetzgebung für den Bereich Datenlogistik auszuarbeiten und bis Ende 2009 Antrag zu stellen.

In die Ausarbeitung des kantonalen Geoinformationsgesetzes (KGIG) wurde der Datenschutzbeauftragte am Rande einbezogen. Er verlangte, dass auf formellgesetzlicher Stufe die notwendige umfassende Regelung für die Bearbeitung und Bekanntgabe von Geodaten und Geoinformationen mit Personenbezug durch kantonale und kommunale öffentliche Organe geschaffen werde. Er verfasste zwei ausführliche Stellungnahmen und erläuterte diese mündlich.

Im Frühling 2009 wurde der Vernehmlassungsentwurf vorgelegt. Von den Vorschlägen des Datenschutzbeauftragten wurden die anfänglich nicht vorgesehene Regelung für die kommunale Geodatenbearbeitung sowie die Schaffung von Rechtsgrundlagen für sachbereichsübergreifende Geoinformationssysteme aufgenommen. Da differenziertere Bestimmungen angezeigt waren, legte der Datenschutzbeauftragte in seiner Stellungnahme zum Vernehmlassungsentwurf erneut Formulierungsvorschläge für den Umgang mit Geodaten, deren Veröffentlichung auf dem Internet zum heutigen und für vergangene Zeitpunkte sowie für den Betrieb von Geoinformationssystemen vor. Er hielt ausserdem fest, dass weder der Vernehmlassungsentwurf noch seine Formulierungsvorschläge es zulassen, dass besondere Personendaten bearbeitet werden. Sollte die Art oder Dichte der zugänglich gemachten Informationen oder die Möglichkeit ihrer Verknüpfung – auch mit Informationen, die nicht dem Geoinformationsgesetz unterstehen – zu einer besonderen Gefahr der Persönlichkeitsverletzung führen, müssten auf formeller Gesetzesstufe viel detailliertere Regelungen als im derzeit diskutierten kantonalen Geoinformationsgesetz geschaffen werden.

Gesetzgebung für die Schulpsychologie

Die Bildungsdirektion will die Schulpsychologie neu organisieren und legt hiezu ein Konzept vor. Weil darin nicht auf den dringend anstehenden Gesetzgebungsbedarf eingegangen wird, gelangte der Datenschutzbeauftragte an die Bildungsdirektion und zeigte die Bereiche mit besonderem Handlungsbedarf auf.

Das Konzept zur Neuregelung der Schulpsychologie beinhaltet hauptsächlich organisatorische Belange. Ausführungen im Bereich der Gesetzgebung fehlen, obwohl die bisherigen Regelungen in der Volksschulgesetzgebung (Volksschulgesetz, Volksschulverordnung, Verordnung über die sonderpädagogischen Massnahmen) nur teilweise erwähnen, ob und wie Personendaten tatsächlich bearbeitet und ausgetauscht werden. Spätestens bis Ende September 2013 bedarf es hinreichend bestimmter Regelungen in einem formellen Gesetz.

Der Datenschutzbeauftragte wies darauf hin, dass im Rahmen einer Gesamtbetrachtung beurteilt werden muss, ob durch die vorgesehene Informationsbearbeitung in Verknüpfung mit anderen Informationen eine besondere Gefahr der Persönlichkeitsverletzung besteht und der Kerngehalt der Grundrechte gewahrt bleibt. Die Bearbeitung von Personendaten muss für die betroffene Person aufgrund der Umschreibung im formellen Gesetz in groben Zügen nachvollziehbar sein. Auf formellgesetzlicher Stufe zu regeln sind deshalb

– der genaue Zweck der Bearbeitung, damit die Verhältnismässigkeit der Datenbearbeitung sowie die Zweckbindung im Einzelfall beurteilt werden können
– die zur Bearbeitung ermächtigten und verantwortlichen Behörden
– die Definition der Aufgaben, Kompetenzen und Verantwortlichkeiten der Schulpsychologinnen und Schulpsychologen
– die Rollen der weiteren, gemäss Volksschulgesetzgebung an den Abklärungen und Beratungen Beteiligten
– die verwendeten Mittel, einschliesslich besondere Regelungen für übergreifende EDV-Systeme
– der Kreis der betroffenen Personen
– die Kategorien der bearbeiteten Daten
– die Voraussetzungen für die Bekanntgabe der bearbeiteten Daten
– die Empfänger und allfällige Abrufverfahren
– die Aufbewahrung der Daten
– die Sicherheitsmassnahmen
– die Rechte der betroffenen Personen und deren Umsetzung.

Ebenso ist zu klären, ob Beschränkungen für die Bearbeitung durch Dritte oder Ausnahmen vom Zugangsrecht nötig sind und ob besondere Schweige- und Geheimnispflichten bestehen oder durchbrochen werden sollen. Diese Anforderungen erlauben es nicht, dass standardisierte, allgemeingültige Formulierungen wie «zu diesem Zweck können auch besondere Personendaten bearbeitet werden» verwendet werden. Es ist darzulegen, welcher Bedarf im Hinblick auf die skizzierten Anforderungen besteht und wie entsprechende Bestimmungen rechtzeitig geschaffen werden können.

Der Datenschutzbeauftragte hat seine Unterstützung bei der Erarbeitung der gesetzlichen Grundlagen angeboten.

Forschung mit Personendaten

In der Forschung werden häufig Personendaten benötigt. Der Datenschutzbeauftragte berät Forschungsinstitutionen und andere öffentliche Organe und erarbeitete ein Merkblatt für häufige Fragen bei Forschungsvorhaben.

Der Datenschutzbeauftragte erhält zunehmend Anfragen im Zusammenhang mit Forschungsprojekten, speziell im Bereich der Medizin- oder Gesundheitsforschung. Sowohl kantonale Institutionen, die schweizweit agieren, als auch verwaltungsinterne Projektteams erkundigen sich nach den datenschutzrechtlichen Rahmenbedingungen für Forschungsprojekte mit Personendaten. So führte beispielsweise ein medizinisches Institut eine Studie über chronische Beeinträchtigungen von Kindern in der Schweiz durch, und eine Universitätsklinik untersuchte die Epidemiologie psychischer Störungen im Kanton Zürich.

Forschungsprojekte, die von öffentlichen Organen des Kantons Zürich durchgeführt werden, müssen die Anforderungen des IDG einhalten. Der Datenschutzbeauftragte berät diese Institutionen, indem er ihnen die datenschutzrechtlichen Leitlinien für das jeweilige Forschungsprojekt erläutert. Die Fragen der Forschungsteams reichten von der Beauftragung Dritter, die einzelne Forschungsschritte übernehmen sollten, über die Erarbeitung einer Einwilligungserklärung der Betroffenen bis zu den organisatorischen und technischen Massnahmen, die eine Forschungsinstitution zum Schutz der Personendaten vorkehren muss.

Weil sich zahlreiche Forscherteams erkundigten, ob und wie sie Personendaten bei den Einwohnerkontrollen beziehen können, hat der Datenschutzbeauftragte dazu das Merkblatt «Personendaten für Forschungsvorhaben» verfasst (www.datenschutz.ch/publikationen). Es zeigt auf, welche Rahmenbedingungen ein Forschungsinstitut einzuhalten hat und wie es vorgehen soll, wenn es diese Daten von einem öffentlichen Organ des Kantons Zürich beziehen will.

Forschende können gestützt auf ein schriftliches Gesuch mit den relevanten Angaben, unter speziellen Bedingungen, Adresslisten von ausgewählten Zielgruppen bei den Einwohnerkontrollen erfragen. Das Forschungsinstitut muss nachweisen, dass die Personendaten im frühestmöglichen Zeitpunkt anonymisiert werden und spätestens nach der Auswertung vernichtet werden. Aus den Auswertungen dürfen keine Rückschlüsse auf betroffene Personen möglich sein. Das Gesuch soll auch die Massnahmen zum Schutz der Personendaten umfassen, vor allem hinsichtlich Zugriff sowie deren Aufbewahrung, Anonymisierung und Vernichtung. Die Personendaten dürfen nur für den bei der Erhebung angegebenen Zweck verwendet und nicht weitergegeben werden.

Anpassungen ans Europarecht

Die europäische Zusammenarbeit in den Bereichen Polizei, Justiz, Visa und Asyl wird fortlaufend ausgebaut und vereinheitlicht. Diese Entwicklung bringt Anpassungen im Datenschutzrecht mit sich, die auch im Schweizer Recht umgesetzt werden müssen.

Die Schweiz ist wegen der Assoziierung an die Abkommen von Schengen und Dublin eng beteiligt an der grenzüberschreitenden polizeilichen und justiziellen Zusammenarbeit. Der zunehmende zwischenstaatliche Datenfluss verlangt nach einem verbesserten und harmonisierten datenschutzrechtlichen (Mindest-)Standard in Europa. Der Datenschutzbeauftragte nahm zum Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten sowie zu zwei weiteren Vernehmlassungen Stellung: Zur Einführung der Biometrie im Ausländerausweis gemäss Schengen-Acquis und zur Umsetzung des von der Schweiz unterzeichneten Übereinkommens des Europarates zur Cyberkriminalität.

Rahmenbeschluss Datenschutz

Der Rahmenbeschluss gilt nur für die Bekanntgabe von Daten im Rahmen der Schengener Zusammenarbeit. Den Schengen-Staaten steht es frei, ihn auch auf ihre nationale Datenverarbeitung anzuwenden. Der nationale Datenschutzstandard sollte grundsätzlich dem im Rahmenbeschluss festgelegten Standard entsprechen.

In einer Stellungnahme wies der Datenschutzbeauftragte darauf hin, dass eine Übertragung der Normen des Rahmenbeschlusses auf die innerstaatliche Datenbearbeitung dort sinnvoll ist, wo allgemeine Grundsätze der Datenbearbeitung betroffen sind und wo in ähnlichen Fällen unterschiedliche Datenschutzstandards angewendet würden. Bei der Datenbeschaffung sei zudem nicht immer feststellbar, ob die Daten danach im Rahmen der Schengener Zusammenarbeit ins Ausland weitergeleitet werden.

Die Normen des Rahmenbeschlusses, die ausschliesslich die Zusammenarbeit zwischen Schengen-Staaten betreffen, werden für den justiziellen Bereich im Strafgesetzbuch (StGB) und für den polizeilichen Bereich im Schengen-Informationsaustausch-Gesetz (SIaG) integriert werden. Dies ist sinnvoll, und es bedarf keiner weiteren Umsetzung auf kantonaler Ebene. Handlungsbedarf sieht der Datenschutzbeauftragte bei den allgemeinen Datenschutzgrundsätzen, die sich nicht spezifisch auf die Schengener Zusammenarbeit beziehen und für die kantonale Datenschutzgesetzgebung keine entsprechenden Regelungen enthält. Er erachtet folgende Bestimmungen als umsetzungsbedürftig:

- Personenbezogene Daten müssen von Amtes wegen berichtigt werden, wenn sie unrichtig sind, und soweit möglich und nötig vervollständigt oder auf den neuesten Stand gebracht werden. Dies ist umso bedeutsamer, sobald Daten zur Übermittlung ins Ausland bereitgestellt werden. Dieser Grundsatz ist in der kantonalen Datenschutzgesetzgebung nur teilweise verwirklicht. Eine Richtigstellung erfolgt nur auf Verlangen der betroffenen Person. Weiter sollen Daten nicht gelöscht, sondern speziell markiert werden, wenn berechtigter Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigen kann.
- Zur Überprüfung der Rechtmässigkeit der Datenverarbeitung wie auch zur Eigenüberwachung und Sicherstellung der Integrität und Sicherheit ist die Übermittlung von Personendaten zu protokollieren oder zu dokumentieren. Die Protokollier- und Dokumentationspflicht sollte im IDG explizit erwähnt werden.

– Die Mitgliedstaaten werden durch den Rahmenbeschluss dazu verpflichtet, dass betroffene Personen im Einklang mit innerstaatlichem Recht über die Bearbeitung ihrer Daten durch die zuständigen Behörden informiert werden. Der Datenschutzbeauftragte schlägt vor, die Bestimmung in § 12 IDG entsprechend anzupassen.
– Im Zusammenhang mit dem Recht auf Berichtigung, Löschung und Sperrung kann der Fall eintreten, dass die Richtigkeit eines personenbezogenen Datums von der betroffenen Person bestritten wird und nicht mehr ermittelt werden kann, ob dieses richtig oder falsch ist. Das betroffene Personendatum sollte entsprechend gekennzeichnet werden. Im aufgehobenen Datenschutzgesetz des Kantons Zürich existierte eine analoge Regelung. Wenngleich die Weisung zum IDG ausführt, dass die heutige und im IDG gekürzte Bestimmung materiellrechtlich an der bisherigen Rechtslage nichts ändere, wäre es der Rechtssicherheit dienlich, diese Bestimmung formell wieder ins IDG aufzunehmen.

Der Regierungsrat nahm die Stellungnahme zur Kenntnis, sieht im Moment aber keine akute Umsetzungsnotwendigkeit.

Biometrie

Schengen-Mitgliedstaaten müssen künftig in den Ausweisen von Drittstaatenangehörigen biometrische Merkmale (Gesichtsbild und zwei Fingerabdrücke) erfassen. Der Datenschutzbeauftragte kritisierte in seiner Stellungnahme, dass der Gesetzesentwurf zum Teil über die Vorschriften der EG-Verordnung hinausgeht. Vorgesehen ist insbesondere, dass die biometrischen Daten zentral gespeichert werden sollen, obschon die EG-Verordnung die Speicherung nur auf dem Datenchip des Ausweises verlangt. Die Gefahren und Risiken einer zentralen Speicherung von biometrischen Daten sind bereits im Vorfeld der Abstimmung über die Einführung der biometrischen Pässe breit diskutiert worden.

Cyberkriminalität

Die Bekämpfung und Verhinderung von Computer- und Netzwerkkriminalität erfordert eine gut funktionierende internationale Zusammenarbeit. Obschon die grenzüberschreitende Weiterleitung von Personendaten und der damit verbundene Eingriff in die Persönlichkeitsrechte der Betroffenen wesentlicher Bestandteil der Konvention bildet, wurde auf die Aufnahme materiellrechtlicher Bestimmungen zum Umgang mit personenbezogenen Daten weitgehend verzichtet. Der Datenschutzbeauftragte kritisiert, dass dadurch die innerstaatlichen Rechtsgarantien zum Schutz von Personendaten teilweise nicht eingehalten werden können.

Sicherheit ist auch Teil der Organisation

Die Kontrollen des Datenschutzbeauftragten decken oft Mängel bei den organisatorischen Massnahmen auf. Diese könnten meist kostengünstiger und wirksamer behoben werden als rein technisch orientierte Detaillösungen.

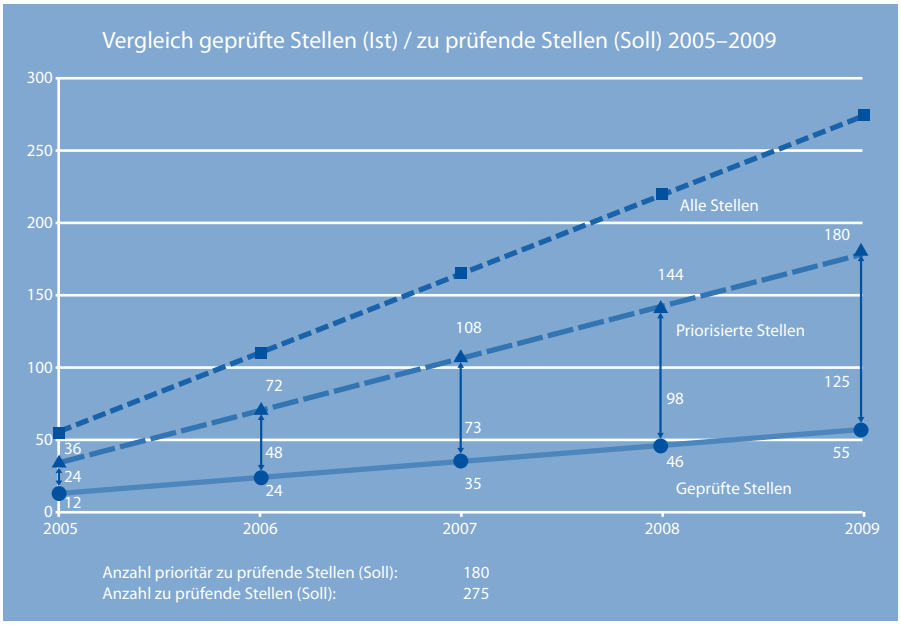
Im Bereich Sicherheit der Informations- und Kommunikationstechnologie (IKT) zeigt sich bei den geprüften Stellen weiterhin, dass unklare oder fehlende strategische Aufträge an die Informatikabteilungen und an die externen Leistungserbringer zu unzureichenden Massnahmen im organisatorischen Bereich führen. So fehlen Rollenkonzepte oder Richtlinien für den Einsatz von mobilen Arbeitsplätzen und -geräten, und die Betriebsdokumentationen sind ungenügend. Die Folgen sind ungenaue Berechtigungsvergaben, unklare Betriebsabläufe oder ungesicherte Daten auf unterschiedlichen mobilen Datenträgern.

Zwar werden die Hinweise und Bemerkungen des Datenschutzbeauftragten im Rahmen der Kontrollen akzeptiert. Trotz einfacher Vorgaben und bewusst kurz gehaltener Massnahmenpläne werden die erforderlichen Aktivitäten indessen oft aufgeschoben.

Neue Prüfungen

Die mit Blick auf das IDG definierten Vorgehensweisen in standardisierte und vertiefte Prüfungen haben sich bewährt (siehe Tätigkeitsbericht Nr. 14 [1.–9.2008], S. 22 f.). Beim Datenschutzreview vom Typ «vertieft» werden Zielsetzungen, Vorgehensweise und Beteiligung der zu prüfenden Stelle klar definiert und schriftlich festgehalten. Die Kontrolle kann so von den Stellen budgetiert, an ihre Bedürfnisse angepasst und gleichzeitig mit der Zielsetzung des Datenschutzbeauftragten abgestimmt werden.

Die Anzahl Prüfungen bewegte sich in der Berichtsperiode im bisherigen Rahmen. Die Verteilung bei den Hauptgruppen (Gemeinden, kantonale Verwaltung und Gesundheitsbereich) blieb unverändert.



Das Intervall zwischen zwei Prüfungen sollte fünf Jahre betragen. «Priorisierte Stellen» sind Organe, die aus Sicht des Datenschutzbeauftragten regelmässig zu überprüfen sind. Um das Fünfjahresintervall einzuhalten, hätten 2009 zusätzlich 122 Stellen geprüft werden sollen.

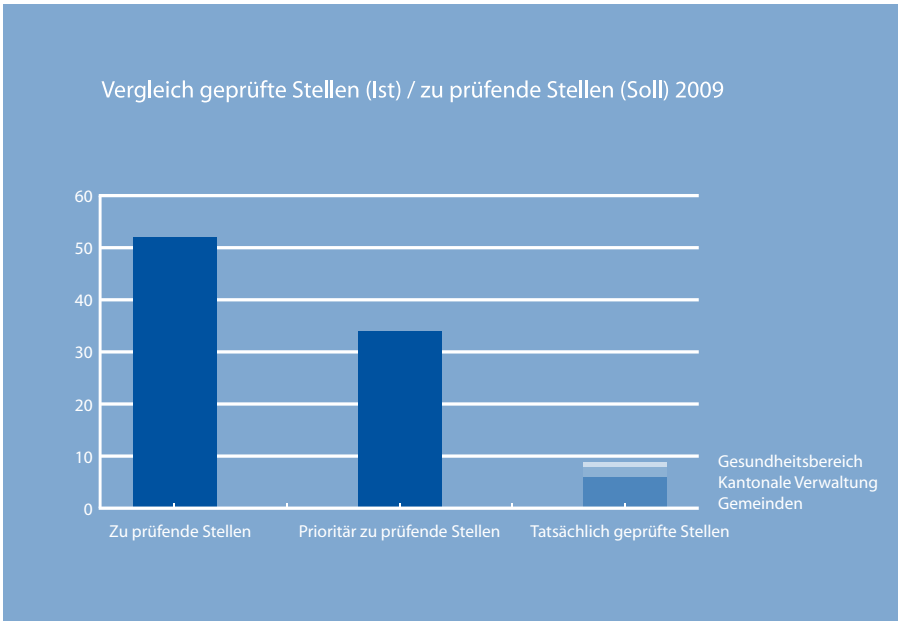
Von Managementsystemen profitieren

In komplexen Umgebungen oder bei Einstufung in Schutzstufe S3 gemäss Informatiksicherheitsverordnung (ISV) sind Managementsysteme für IKT-Sicherheit unverzichtbar, um die bestehenden Ressourcen wirksam zur Risikoverminderung einzusetzen. Die entsprechenden Standards wie der internationale Standard ISO/IEC 27001:2005 oder der lokale Standard des Bundesamts für Sicherheit in der Informationstechnik BSI 100-1 werden noch immer zu wenig verwendet. Damit könnten Defizite besser erkannt und ein angemessenes Sicherheitsniveau in allen Bereichen erreicht werden.

Neben den technischen Aspekten sind die organisatorischen Massnahmen zu verbessern. Sowohl die Führungsebene als auch die Mitarbeitenden müssen involviert werden: Es ist Aufgabe der Führung, die notwendigen Arbeiten zu fordern, zu unterstützen und die notwendigen Ressourcen bereitzustellen, damit die organisatorischen Handlungsanweisungen umgesetzt werden können.

Detaillierte Rollen- und Berechtigungskonzepte sind immer noch selten. Solche Dokumente minimieren den Verwaltungsaufwand, vermeiden Doppelspurigkeiten und schaffen Transparenz und klare Verhältnisse – auch in Bezug auf die Aufträge an die externen Dienstleistenden.

Die IKT-Abteilungen können mit klaren Anforderungen aus den Fachabteilungen die Daten der Bürgerinnen und Bürger so schützen, dass das Vertrauen in die Verwaltung auch berechtigt ist. Die Managementsysteme und organisatorischen Leitplanken helfen dort Zeit und Geld einzusetzen, wo sie am meisten gebraucht werden.



Tatsächlich geprüfte Stellen 2009

Gemeinden	6
Kantonale Verwaltung	2
Gesundheitsbereich	1
Total	**9**

Kontrolle des Staatsschutzes

Das Bundesgesetz zur Wahrung der inneren Sicherheit sieht vor, dass kantonale Polizeiorgane Staatsschutzaufgaben wahrnehmen. Soweit diese kantonalen Behörden Personendaten bearbeiten, unterliegen sie der Aufsicht des Datenschutzbeauftragten.

Die Wahrung der inneren Sicherheit ist gleichzeitige Aufgabe des Bundes und der Kantone. Jeder Kanton bestimmt eine Vollzugsbehörde, die in diesem Bereich mit den Behörden des Bundes zusammenarbeitet. Im Kanton Zürich werden die staatsschutzrelevanten Aufgaben durch die Kantons- und die Stadtpolizei erfüllt. Die datenschutzrechtliche Aufsicht ist in der Datenbearbeitung der betroffenen Organe begründet. Der Datenschutzbeauftragte hat deshalb im Jahr 2009 eine datenschutzrechtliche Kontrolle bei der Kantonspolizei eingeleitet.

Die Aufsicht der kantonalen Datenschutzbeauftragten in diesem Bereich ist nicht unumstritten. Obwohl das Bundesgesetz zur Wahrung der inneren Sicherheit (BWIS) die Aufsichtsrechte gemäss kantonalem Recht vorbehält, beansprucht der Bund diese Kontrolltätigkeit auch für sich. Er bezieht sich unter anderem auf die Verordnung des BWIS, wonach nur unter Zustimmung des Staatsschutzorgans Einsicht in die Bundesdaten genommen werden kann. Unbestritten ist jedoch, dass die Verwaltungskontrolle, also die Dienstaufsicht, durch die hierarchisch übergeordnete Behörde wahrgenommen werden soll; die parlamentarische Kontrolle dagegen kann sowohl vom Bund als auch, obwohl im Gesetz nicht geregelt, von den Kantonen ausgeführt werden. Auch die Kontrolle der Verwaltungsabläufe durch die kantonalen Datenschutzbeauftragten wird nicht in Frage gestellt.

Die Einschränkung der kantonalen datenschutzrechtlichen Aufsicht in Bezug auf den Umfang der einzusehenden Daten ist in diesem sensitiven Bereich der Datenbearbeitung problematisch. Die Rechtmässigkeit der Datenbearbeitung kann ohne volle Einsicht nicht umfassend kontrolliert werden. In anderen Kantonen werden nun weitere Aufsichtsmodelle diskutiert, beispielsweise die Schaffung einer neuen Kommission, die gemeinsam mit den Datenschutzbeauftragten die Bearbeitung von Staatsschutzdaten kontrollieren soll. Die Aufsichtsstruktur muss in jedem Fall zügig überprüft und geregelt werden, um einen aufsichtsfreien Raum zu verhindern.

Die Regelung dieser aufsichtsrechtlichen Frage ist von nationaler Relevanz. Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, befasst sich deshalb mit diesem Thema: Mit einem Fragebogen wurden die Staatsschutztätigkeiten in den einzelnen Kantonen evaluiert. Die Auswertung bei elf Kantonen zeigt, wie unterschiedlich die Organisation und die Tätigkeiten des Staatsschutzes gestaltet sind. Der Umfang und die Art und Weise der datenschutzrechtlichen Kontrollen werden diese unterschiedlichen Ansätze des Staatsschutzes berücksichtigen müssen.

Privatheit wird zum Thema

Weil die Privatheit zunehmend bedroht ist, nimmt die Nachfrage nach datenschutzrechtlichen Informationen verstärkt zu. Der Datenschutzbeauftragte greift die vordringlichen Aspekte zum Schutz der Privatheit auf und informiert darüber auch mittels Kooperationen.

Die Nachfrage nach datenschutzrechtlicher Information steigt weiter: Speziell die neuen technologischen Möglichkeiten und Dienstleistungen in den Bereichen Internet und Überwachung werfen zunehmend Fragen auf nach der Vereinbarkeit mit dem Grundrecht auf Privatheit. So hat nicht nur die Zahl der Anfragen und Beschwerden von Bürgerinnen und Bürgern stark zugenommen; deutlich grösser als in den Vorjahren ist auch die Nachfrage der Medien. Bei den öffentlichen Organen haben besonders die Neuerungen durch das IDG zusätzliche Fragen zur Umsetzung aufgeworfen. Und die Nachfrage nach Gastreferaten ist gegenüber den Vorjahren nochmals deutlich gestiegen.

Nachfrage gezielt abdecken

Der Datenschutzbeauftragte kommt dem zunehmenden Informationsbedarf, priorisiert nach Wirkung, so weit wie möglich nach, unter anderem mit folgenden Massnahmen:

- Das IDG sieht vor, dass beabsichtigte Datenbearbeitungen rechtzeitig auf die Vereinbarkeit mit dem Datenschutz geprüft werden. Anhand des Merkblatts «Vorabkontrolle» können öffentliche Organe einfach klären, ob und wie sie geplante Datenbearbeitungen zur Vorabkontrolle melden müssen (www.datenschutz.ch/publikationen).
- Die Sozialbehörden äusserten Klärungsbedarf über den Umgang mit ihren sensiblen Informationen. Die datenschutzrechtlichen Voraussetzungen werden nun im Leitfaden «Datenschutz im Sozialbereich» praxisnah erläutert (www.datenschutz.ch/publikationen).
- Weil Forschungsinstitute zunehmend Personendaten benötigen, erläutert das Merkblatt «Personendaten für Forschungsvorhaben», wann und wie sie diese von einem öffentlichen Organ des Kantons Zürich beziehen können (www.datenschutz.ch/publikationen).
- Betroffene und interessierte Personen und Institutionen können vom umfangreichen Informations- und Unterstützungsangebot auf der neuen Website nun noch einfacher profitieren (www.datenschutz.ch).

Kommunizieren und befähigen

Der Datenschutzbeauftragte greift auch vordringliche datenschutzrechtliche Aspekte auf. Eine aktive Informationspolitik erforderte weiterhin das Gesundheitswesen. Einen weiteren Kommunikationsschwerpunkt bildeten die neuen Möglichkeiten des Internets auch für öffentliche Organe.

Damit datenbearbeitende Stellen und Personen den Datenschutz in ihrem Wirkungskreis selbständig sicherstellen können, führte der Datenschutzbeauftragte weitere Seminare im Rahmen seines Aus- und Weiterbildungsangebots durch.

Wirkung verstärken

Für eine grössere Wirkung bei ausgewählten datenschutzrechtlichen Themen pflegt der Datenschutzbeauftragte bewährte Kooperationen: In Zusammenarbeit mit Privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, führte er die erste repräsentative Studie zu «Datenschutz in der Schweiz» durch, die er anlässlich des 3. Europäischen Datenschutztages präsentierte. Die Studie löste ein grosses Echo nicht nur in der Öffentlichkeit, sondern auch bei den untersuchten Industrien aus. In Zusammenarbeit mit der Stiftung für Datenschutz und Informationssicherheit veranstaltete er das «14. Symposium on Privacy and Security 2009» zum Thema «Internet mit neuen Dimensionen» für Entscheidungsträger aus Wirtschaft, Verwaltung und Politik. Der erneut grosse Anklang dieser Veranstaltung bestätigt das Interesse an datenschutzrechtlichen Themen auch in dieser Form.

Wirkung des Gesetzes

In der Einführungsphase des IDG ist es noch verfrüht, in Bezug auf die Wirkung des Gesetzes Schlussfolgerungen zu ziehen. Erste Angaben können Grundlage für die systematische Analyse bilden.

Die Berichterstattung des Datenschutzbeauftragten beinhaltet auch die Wirkung des Gesetzes (§ 39 IDG). Die Wirkung des Gesetzes ist an dessen Zielsetzungen zu messen: Das IDG regelt den Umgang der öffentlichen Organe mit Informationen unter zwei Aspekten:

– das Handeln der öffentlichen Organe ist transparent zu gestalten, so dass die freie Meinungsbildung, die Wahrnehmung der demokratischen Rechte und die Kontrolle des staatlichen Handelns erleichtert werden;
– das Bearbeiten von Informationen hat die Grundrechte der betroffenen Personen zu schützen.

Damit sind einerseits das Öffentlichkeitsprinzip respektive der Informationszugang und andererseits die persönliche Freiheit respektive der Datenschutz angesprochen. In beiden Fällen geht es somit um die Gewährleistung und den Schutz von demokratischen und verfassungsmässig garantierten Rechten von Bürgerinnen und Bürgern. Der Datenschutzbeauftragte hat dabei die Rolle eines unabhängigen Vermittlers, der sich für die Gewährleistung dieser Rechte einsetzt (allerdings nicht in Bezug auf das Öffentlichkeitsprinzip, da ihm hierfür die entsprechende Funktion nicht übertragen wurde).

Die Betrachtung der Wirkung des Gesetzes umfasst die verschiedenen Instrumente des IDG zur Gewährleistung des Informationszugangs respektive des Datenschutzes. In der vorliegenden Berichterstattung wird auf eine systematische Auseinandersetzung verzichtet: Die Einführungsphase eines Gesetzes hat ihre eigene Typologie, da sie für alle beteiligten Stellen einen besonderen Aufwand bedeutet, wie die Schwerpunkte und Feststellungen im vorliegenden Tätigkeitsbericht zeigen. Allerdings liegen in verschiedenen Bereichen schon heute Angaben vor, die später in eine systematische Betrachtung einfliessen können.

Im Bereich des Informationszugangs führt die Koordinationsstelle IDG der Staatskanzlei eine Statistik über die Anzahl entsprechender Gesuche und deren Behandlung. Diese Zahlen werden im Geschäftsbericht des Regierungsrates veröffentlicht. Diese Statistik umfasst aber lediglich die kantonale Verwaltung.

Der Datenschutzbeauftragte legt im Rahmen des konsolidierten Entwicklungs- und Finanzplans (KEF) leistungs- und wirkungsorientierte Indikatoren fest. Im Berichtsjahr wurden diese auf die Erfordernisse des IDG ausgerichtet (siehe folgende Seite). Des Weiteren besitzt der Datenschutzbeauftragte ein Qualitätsmanagementsystem, das nach ISO 9001 zertifiziert und auf die wirkungsorientierte Erfüllung der Aufgaben und Funktionen ausgerichtet ist. Hierfür wurden entsprechende Prozesse definiert.

Für die systematische Darstellung der Wirkung des Gesetzes werden diese bestehenden Hilfsmittel eine Grundlage bilden. Für die Berichterstattung in den folgenden Jahren werden entsprechende Analyse- und Beurteilungsinstrumente zu evaluieren sein. Auf solchermassen gesicherten Grundlagen wird es sodann möglich sein, die Wirkung des Gesetzes zu diskutieren und allenfalls Massnahmen zu treffen. Hierbei werden nicht nur die öffentlichen Organe, sondern auch der Gesetzgeber angesprochen sein.

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 07	B 08	Δ(P 09)	P 09	Δ(P 10)	P 10	Δ(P 11)	P 11	P 12	Δ%(07-12)
Ertrag	0.2	0.2	0.0	0.2	0.0	0.2	0.0	0.0	0.0	-83.4
Aufwand	-1.7	-1.9	0.0	-2.1	0.0	-2.2	0.0	-2.2	-2.2	32.7
- Personalaufwand		-1.2		-1.4		-1.4		-1.5	-1.5	
Saldo	-1.5	-1.8	0.0	-1.9	0.0	-2.0	0.0	-2.2	-2.2	

Investitionen (in Mio. Fr.)										Ø (07 -12)
Einnahmen										
Ausgaben	-0.3		0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.0
Nettoinvestitionen	-0.3		0.0	0.0	0.0	0.0	0.0	0.0	0.0	-0.0
Personal (Beschäftigungsumfang)	7.2	7.2	0.0	8.2	0.0	8.2	0.0	8.2	8.2	

Aufgaben

A1 Der Datenschutzbeauftragte beaufsichtigt die Datenbearbeitungen der kantonalen Verwaltung, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton. Er stellt sicher, dass die Privatheit der Bürgerinnen und Bürger respektiert wird.
A2 Er führt Kontrollen durch, beurteilt datenschutzrelevante Vorhaben und Erlasse, berät die verantwortlichen Organe und fördert den Einsatz datenschutzfreundlicher Technologien. Dabei kann er verbindliche Empfehlungen abgeben.
A3 Der Datenschutzbeauftragte informiert und sensibilisiert die Öffentlichkeit für die Anliegen des Datenschutzes und der Informationssicherheit. Er berät Privatpersonen und vermittelt in Konfliktfällen.
A4 Alle Aufgaben nimmt der Datenschutzbeauftragte in vollständiger Unabhängigkeit wahr.

Entwicklungsschwerpunkte

		bis	Direktions-ziel Nr.
E1	Vorabkontrolle: Detailkonzeption und Aufbau	2009	0
E2	Aufsicht: Verstärkung durch Aufbau eines Monitorings (konzeptionelle Weiterentwicklung und Standardisierung der Prozesse)	2011	0
E3	Besondere Personendaten: Verstärkung von Aufsicht und Kontrolle im Gesundheitswesen sowie im Bereich Polizei und Strafuntersuchung	2009	0
E4	Datenschutzfreundliche Technologien: Förderung der Entwicklung und des Einsatzes von datenschutzfreundlichen Technologien	2011	0

Indikatoren

	Art	R 07	B 08	P 09	P 10	P 11	P 12
Wirkungen							
W1 Anteil umgesetzter Empfehlungen	P			60 %			
W2 Kundenbeurteilung der Qualität der Leistungen	min.			gut			
W3 Anteil umgesetzter Hinweise	P			60 %			
Leistungen							
L1 Anteil komplexer Beratungen von öffentlichen Organen	P			33 %			
L2 Anteil aufwändiger Beratungen von Privatpersonen	P			15 %			
L3 Anzahl Grundsatzfragen u. Stellungnahmen				25			
L4 Anzahl Datenschutz-Reviews				20			
L5 Zuwachs Besuche auf Internetangeboten	P			5 %			
L6 Anzahl Teilnehmerstunden an Weiterbildungsangeboten				600			
Wirtschaftlichkeit							

Leistungsgruppe 9071	Budgetentwurf 2009
Budgetkredit Erfolgsrechnung (in Mio Fr.)	-1.940
Budgetkredit Investitionsrechnung (in Mio. Fr.)	0.000

Budget	Leistungsgruppe 9071
Vom Budgetentwurf abweichende Budgetbeschlüsse des KR können hier eingeklebt werden	

Anhang 1-10

Strommessung mit Smart Meters

Die automatisierte Stromverbrauchsmessung bei Privathaushalten mit Smart Meters stellt eine Bearbeitung von Personendaten dar. Die viertelstündliche Messung des Energieverbrauchs birgt das Risiko, dass diese Daten anderen Nutzungsmöglichkeiten zugeführt und Persönlichkeitsprofile erstellt werden können. Transparenz, Zweckbindung und Verhältnismässigkeit sind deshalb besonders zu beachten. Damit Smart Meters flächendeckend eingeführt werden können, muss der Zweck mindestens in einer Verordnung festgehalten werden.

§ 2 EKZ-Gesetz

Die Elektrizitätswerke des Kantons Zürich (EKZ) unterbreiteten dem Datenschutzbeauftragten ein Pilotprojekt zur automatisierten Strommessung in Privathaushalten mit intelligenten Zählern (Smart Meters) zur Vorabkontrolle (siehe auch Seite 12). Ziele des Pilotprojekts sind die automatisierte Messung des Stromverbrauchs und deren Übermittlung an die EKZ. Zudem sollen die monatliche Rechnungsstellung an die Privathaushalte und eine präzise Bestimmung der Stromlastspitzen erzielt werden, wodurch die gesamte Energieeffizienz erhöht werden soll. Die Smart Meters zeichnen dazu viertelstündlich die Stromverbrauchsmessungen auf. Im gleichen Rhythmus werden die Messwerte elektronisch erfasst und im Internet verschlüsselt übermittelt.

Im Rahmen des automatisierten Messsystems werden nicht nur Personendaten bearbeitet; es besteht auch die Möglichkeit, Persönlichkeitsprofile zu erstellen: Die Energienutzung in Privathaushalten widerspiegelt Tagesabläufe. Indem der Lastgang viertelstündlich gemessen und der punktgenaue Energieverbrauch abgelesen werden können, lässt sich auf die Gewohnheiten der Betroffenen schliessen. Elektronisch erfasste Energieverbrauchsdaten einer Person können unbegrenzt gespeichert und jederzeit abgerufen werden. Dies führt dazu, dass diese Personendaten somit auch anderen Nutzungsmöglichkeiten zugeführt und allenfalls auch Persönlichkeitsprofile erstellt werden könnten. Für die Persönlichkeitsrechte der betroffenen Personen stellt dies ein erhebliches Risiko dar.

Normalerweise erfüllt bereits eine Aufgabenumschreibung in einer Verordnung die gesetzliche Anforderung an das Bearbeiten von Personendaten. Die EKZ haben für das Pilotprojekt eine ausreichende gesetzliche Grundlage: Sie umschreibt, dass die EKZ eine wirtschaftliche, sichere und umweltgerechte Energieversorgung gewährleisten müssen. Weil jedoch die Möglichkeit zum Erstellen von Persönlichkeitsprofilen besteht, müssen bei der Umsetzung des Projektes Verhältnismässigkeit, Zweckbindung und Transparenz besonders beachtet werden.

Weil die automatisierte Messung verhältnismässig sein muss, erscheint das vorgesehene viertelstündliche Messintervall für eine monatliche Rechnungsstellung an die Privathaushalte als möglicherweise unverhältnismässig kurz. Der Datenschutzbeauftragte riet den EKZ daher, eine Verlängerung der Messintervalle sowohl in Bezug auf die monatliche Rechnungsstellung als auch auf den Gesamtenergieverbrauch zu prüfen. Mit Blick auf eine mögliche Erstellung von Persönlichkeitsprofilen hielt er zudem fest, dass die Zweckbindung der Datenerhebung ausdrücklich in einer gesetzlichen Grundlage festzuhalten sei, wenn die Smart Meters flächendeckend eingeführt werden sollen. Eine entsprechende Verordnungsbestimmung sei ausreichend.

Schulbeurteilung im Internet

Berichte über die Qualität der Schulen in pädagogischer und organisatorischer Hinsicht können auf dem Internet veröffentlicht werden, soweit sie keine Informationen enthalten, die einer bestimmbaren Person zugeordnet werden können. Dies kann durch Anonymisierung erreicht werden oder indem die Rahmenbedingungen einer Funktion beurteilt werden – und nicht die Person, die diese Funktion wahrnimmt.

Die Fachstelle für Schulbeurteilung hat den Auftrag, die Qualität der Schulen in pädagogischer und organisatorischer Hinsicht mindestens alle vier Jahre zu prüfen. Sie erhebt zu diesem Zweck umfangreiche Informationen durch eigene Beobachtungen, schriftliche Befragungen, Interviews sowie anhand verschiedener Unterlagen. Viele dieser teilweise sensitiven Informationen können Lehrern, Schulleiterinnen oder anderen Personen zugeordnet werden. Gestützt auf diese Informationen verfasst die Fachstelle für Schulbeurteilung einen Bericht und schlägt Massnahmen zur Qualitätssicherung vor.

Die Fachstelle möchte den vollständigen Evaluationsbericht nicht nur der jeweiligen Schule und Schulpflege, sondern allgemein via Internet zugänglich machen. Der Bericht darf deshalb keine Informationen enthalten, die jemandem zugeordnet werden können. Sachverhalte und Aussagen müssen dazu so beschrieben werden, dass daraus keine Einzelpersonen mehr bestimmbar sind, und Personen müssen entsprechend in Gruppen zusammengefasst werden. Insbesondere in Bezug auf die Schulleitung, welche häufig aus einer Einzelperson besteht, ist eine solche Anonymisierung nicht möglich. Deshalb dürfen nur Aussagen zu den Rahmenbedingungen solcher Funktionen gemacht werden und keinesfalls dazu, wie diese Funktion durch eine Person wahrgenommen wird.

Für die Qualifikation als Personendatum ist es unerheblich, ob die Information für die Person positiv oder negativ ist. Es spielt auch keine Rolle, ob es sich um eine im Bericht festgehaltene Beurteilung der Fachstelle oder um eine darin zitierte Aussage Dritter handelt. Eine betroffene Person kann nur einwilligen, dass der Bericht veröffentlicht wird, wenn diese Einwilligung im Ausnahmefall, und nicht routinemässig, eingeholt wird. Wegen des Abhängigkeitsverhältnisses dürfte die erforderliche Freiwilligkeit für eine Einwilligung zudem in vielen Fällen nicht gegeben sein.

Besteht ein Bedürfnis, in den Evaluationsberichten auch Personendaten nicht nur der Schule und der Schulpflege zugänglich zu machen, muss die heutige, im Volksschulgesetz verankerte Regelung geändert und eine hinreichend bestimmte Rechtsgrundlage für die Publikation im Internet geschaffen werden. Der Datenschutzbeauftragte hat der Fachstelle für Schulbeurteilung diese Auskünfte aufgrund ihrer Anfrage erteilt.

Beurteilung von Lehrveranstaltungen

Die systematische Beurteilung von Lehrveranstaltungen stellt einen erheblichen Eingriff in die Persönlichkeitsrechte der betroffenen Dozierenden dar. Ein Reglement der Universität regelt den Ablauf des Lehrbeurteilungsprozesses hinreichend transparent und gewährleistet, dass die betroffenen Dozierenden ihre Rechte wahrnehmen können.

§ 20 Abs. 2 und § 21 IDG
§ 39 Abs. 1 und 2 Personalgesetz
§ 8 Abs. 1 IDG
§ 20 Abs. 1 IDG

Die Universität ersuchte den Datenschutzbeauftragten zu prüfen, ob das Reglement über die Beurteilung von Lehrveranstaltungen mit den Anforderungen des Datenschutzes vereinbar sei. Mit der Lehrveranstaltungsbeurteilung, einem universitätsinternen Evaluationsinstrument, soll die Lehrqualität an der Universität gesichert und verbessert werden. Sie soll sowohl den kontinuierlichen Austausch zwischen Studierenden und Dozierenden sicherstellen als auch Dozierende und Lehrverantwortliche zur Diskussion über die Lehre anregen. Gleichzeitig sollen mit dem Reglement die bisher je nach Lehrstuhl unterschiedlichen Beurteilungen vereinheitlicht und konsequent elektronisch durchgeführt werden.

Die Beurteilung von Lehrveranstaltungen bedeutet einen erheblichen Eingriff in die Persönlichkeitsrechte der betroffenen Dozierenden. Weil das Reglement eine Bewertung von Lehrveranstaltungen ohne Einverständnis der betroffenen Dozierenden vorsieht, ist sie ausreichend transparent zu regeln. Für die betroffenen Dozierenden muss in groben Zügen nachvollziehbar sein, wie ihre Personendaten bearbeitet werden, so zum Beispiel, welche Stelle der Universität welche Personendaten der Dozierenden im Lehrbeurteilungsprozess bearbeitet und an welche andere Stelle sie diese weitergeben darf. Ferner dürfen im Rahmen dieser Beurteilung nur Angaben erhoben werden, die für die Sicherung und Entwicklung der Lehrqualität geeignet und erforderlich sind. Zugriff auf nicht anonymisierte Befragungsergebnisse sollen nur jene Angestellten der Universität erhalten, die diese für die gesetzlich umschriebene Aufgabenstellung benötigen. Die personenbezogenen Befragungsergebnisse sind während der Nutzungsdauer gegen unbefugten Zugriff zu sichern und danach zu löschen. Die Universität hat den betroffenen Dozierenden ihre Rechte, wie das Auskunfts- und Berechtigungsrecht, zu gewähren. Als Arbeitgeberin ist die Universität auch im Rahmen von Lehrveranstaltungsbeurteilungen verpflichtet, die Dozierenden in ihrer Persönlichkeit zu schützen.

Je nach Ausgestaltung der Fragebogen stellen die Ergebnisse der Befragung besondere Personendaten über die betroffenen Dozierenden dar. Bezieht sich die Befragung auf den Charakter und das Verhalten der Dozierenden, werden wesentliche Aspekte ihrer Persönlichkeit beurteilt. Die regelmässige Bearbeitung solcher besonderen Personendaten ist nur gestützt auf eine hinreichend bestimmte formellgesetzliche Regelung zulässig. Das Reglement über die Lehrveranstaltungsbeurteilung ist dafür nicht ausreichend. Die Lehrveranstaltungsbeurteilungen gelten zudem als von der Universität bearbeitete amtliche Informationen, die aufgrund des Öffentlichkeitsprinzips jedermann zugänglich sind. Das individuelle Informationszugangsrecht kann nicht auf Stufe eines Reglements, sondern nur auf formellgesetzlicher Stufe generell ausgeschlossen werden.

Die Universität berücksichtigte die Ausführungen des Datenschutzbeauftragten. Das Reglement über die Beurteilung von Lehrveranstaltungen durch die Studierenden an der Universität, das am 14. September 2009 in Kraft getreten ist (LS 415.121), genügt damit den datenschutzrechtlichen Anforderungen.

Absenzen in Schulzeugnissen

Absenzeneinträge in Schulzeugnissen sind Personendaten, unter Umständen sogar besondere Personendaten. Um die Absenzen in die Zeugnisse einzutragen, bedarf es deshalb einer hinreichend bestimmten Regelung in einem formellen Gesetz, wobei Zweck und Umfang der Einträge festzulegen sind.

Gemäss den Bestimmungen der Volksschulgesetzgebung werden Schülerinnen und Schüler der Primar- und Sekundarstufe regelmässig beurteilt. Das Zeugnisreglement sieht eine vierstufige Beurteilung des Arbeits- und Lernverhaltens vor. Unter der Rubrik «Erscheint pünktlich und ordnungsgemäss zum Unterricht» können unentschuldigte Absenzen erfasst werden, soweit sie auf das Verhalten des Schülers oder der Schülerin zurückzuführen sind. Allfällige Pflichtverstösse der Eltern werden im Zeugnis nicht erfasst. Genauere Angaben zum Umfang unentschuldigter Absenzen können nur als ausserordentliche Bemerkungen im Lernbericht, der im Zeugnis nicht erwähnt wird, festgehalten werden. Entschuldigte und unentschuldigte Absenzen dürfen höchstens im Ausnahmefall im Zeugnis unter «Bemerkungen» zu den einzelnen Fachleistungen Eingang finden, wenn sie die Ursache für einzelne Noten oder für auffällige Veränderungen in den Leistungen sind. Auch in Bezug auf Fachleistungen ist der Lernbericht das Gefäss für weiter gehende Angaben zur Schulpräsenz.

Der Datenschutzbeauftragte wies in einer Stellungnahme an das Volksschulamt darauf hin, dass unentschuldigte und entschuldigte Absenzen (in Zusammenhang mit einer Krankheit) besondere Personendaten sein können. Für Bearbeitung und Bekanntgabe solcher Daten ist eine hinreichend bestimmte Regelung in einem formellen Gesetz notwendig. Zeugnis und Lernbericht werden den Erziehungsberechtigten ausgehändigt. Während der Lernbericht Dritten nicht zur Kenntnis gegeben werden muss, wird das Zeugnis bei Bewerbungen für Lehr- oder Arbeitsstellen oder Ausbildungen verlangt. Für eine systematische und quantifizierte Erfassung von Absenzen in Zeugnissen reichen die geltenden Bestimmungen nicht aus. Aus der erforderlichen formellgesetzlichen Grundlage muss hervorgehen, zu welchem Zweck Absenzen erfasst werden sollen und welche genaueren Angaben dazu geeignet und erforderlich sind. Dabei wäre eine Unterscheidung zwischen entschuldigten und nicht entschuldigten Absenzen im Zeugnisformular sinnvoll, weil das Risiko einer Persönlichkeitsverletzung bei unentschuldigten Absenzen ungleich höher ist.

Fehlbares Verhalten von Schülerinnen oder Schülern könnte jedoch auch anderweitig geahndet werden, beispielsweise in einer entsprechenden Rubrik beim Beschrieb des Arbeits- und Lernverhaltens oder in einem zusätzlichen Dokument (Lernbericht). Der Datenschutzbeauftragte verweist auf die vorhandenen Möglichkeiten, soweit unter «fehlbarem Verhalten» unentschuldigte Absenzen, die auf das Verhalten des Schülers zurückzuführen sind, verstanden werden. Im Rahmen der vierstufigen Beurteilung des Arbeits- und Lernverhaltens sowie des Sozialverhaltens könne auch anderes allfälliges fehlbares Verhalten in das Zeugnis einfliessen; im Lernbericht sei eine detailliertere Beschreibung möglich.

Vielfältige Verwendung der UZH Card

Die UZH Card, ein Ausweis der Universität für Studierende und Angestellte, verfügt über einen RFID-Chip und kann vielfältig eingesetzt werden. Randdaten, die zur Aufgabenerfüllung nicht notwendig sind, dürfen nicht weiterverwendet werden. Die Weitergabe von Personendaten an Dritte für die Nutzung der Karte im ausseruniversitären Bereich ist mit Einwilligung der betroffenen Personen möglich.

§ 11 IDG

Die UZH Card soll von Studierenden der Universität zur Identifikation im Hochschulumfeld, als Ausweis in den Bibliotheken und zur Benützung der Sportanlagen verwendet werden. Die Karte soll künftig auch Vergünstigungen ausserhalb der Universität ermöglichen, namentlich die Benützung von Mobility-Fahrzeugen. Für Mitarbeitende soll die UZH Card als Personalausweis dienen – mit den gleichen Möglichkeiten wie für Studierende. Der obligatorische Ausweis weist visuelle und elektronische Merkmale zur Identifizierung der Angehörigen der Universität auf. Damit er kompatibel ist mit bereits bestehenden Schliesssystemen von Universitätsgebäuden, wurde ein RFID-Chip (Radio Frequency Identification) in die Karte integriert. Auf dem Chip befinden sich keine persönlichen Daten. Die UZH Card soll bald als Badge den Zutritt zu gewissen Gebäuden ermöglichen.

Nach Durchsicht des Konzepts wies der Datenschutzbeauftragte auf ungeklärte Fragen zu sogenannten Randdaten hin, also Personendaten, die zur Aufgabenerfüllung nicht notwendig sind. Datenbearbeitungssysteme und -programme sind so zu gestalten, dass möglichst wenig Randdaten anfallen. Randdaten sind zu löschen, zu anonymisieren oder zu pseudonymisieren, sobald und soweit dies möglich ist. Die Hinweise des Datenschutzbeauftragten im Hinblick auf den Umgang mit Randdaten wurden durch die Universität umgesetzt.

Im Weiteren wies der Datenschutzbeauftragte die Universität darauf hin, dass keine Daten von Universitätsangehörigen im Zusammenhang mit der Mobility-Mitgliedschaft bearbeitet werden dürfen. Die Einwilligungserklärung der Studierenden berechtige die Universität, deren Daten einmalig an Mobility weiterzugeben, liesse aber keinen weiteren Datenaustausch zwischen der Universität und Mobility zu. Dies gelte beispielsweise auch bei einem Verlust der UZH Card. Die Universität bestätigte dem Datenschutzbeauftragten, dass dessen Vorgaben in der Zusammenarbeit mit Mobility berücksichtigt würden.

Abstimmungsunterlagen im Internet

Geschäfte von Gemeindeversammlungen, die Personendaten enthalten, dürfen publiziert werden, wenn die Personendaten für die stimmberechtigten Gemeindemitglieder geeignet und erforderlich sind. Eine Bekanntgabe an einen weiteren Adressatenkreis – insbesondere über das Internet – erfordert eine hinreichend bestimmte Rechtsgrundlage, welche die Internetpublikation ausdrücklich vorsieht.

§ 43 Abs.1 GG

Eine Gemeinde veröffentlichte im Weisungsheft Erläuterungen und Empfehlungen zu einem Kaufvertrag der Reformierten Kirchgemeinde. Der Kaufvertrag über ein Grundstück, das von der Kirchgemeinde erworben werden soll, enthielt Name und Adresse der Verkäufer sowie Details über bestehende Hypotheken und zur Bankverbindung. Die Gemeinde veröffentlichte das Weisungsheft auf ihrer Website als abrufbare Datei und anschliessend auch den Abstimmungsbeschluss.

Veröffentlichungen im Zusammenhang mit kommunalen Wahlen und Abstimmungen sind im Gemeindegesetz geregelt: Verhandlungsgegenstände sind den Stimmberechtigten mindestens zwei Wochen vor der Versammlung zur Einsicht aufzulegen. Mit dieser Bestimmung besteht zwar eine Rechtsgrundlage für die Bekanntgabe von Personendaten an stimmberechtigte Gemeindemitglieder. Dennoch muss für jedes Geschäft geprüft werden, welche Information für die unverfälschte Willensbildung der Stimmberechtigten geeignet und erforderlich sind. Die Bestimmung regelt nur die Information zuhanden der Stimmberechtigten, ist indessen keine Ermächtigung für die Bekanntgabe von Personendaten an einen weiteren Adressatenkreis. Obwohl Kirchgemeinden ihre Wahl- und Abstimmungsleitung an die politischen Gemeinden delegieren können, dürfen ihre Abstimmungsgegenstände, sobald sie Personendaten enthalten, nicht zur Kenntnis der gesamten politischen Gemeinde gelangen.

Weil Informationen, die im Internet veröffentlicht sind, unkontrolliert weiterverbreitet werden können, bedeutet eine Publikation von Personendaten auf einer Website einen besonderen Eingriff in die Persönlichkeitsrechte. Eine rechtliche Bestimmung ist deshalb nur dann eine hinreichend bestimmte Rechtsgrundlage für eine Internetpublikation, wenn sie ausdrücklich auf diese Publikationsform verweist. Generalklauseln wie die Erwähnung von «geeigneten Mitteln» der Publikation sind ungenügend. Das Publikationsgesetz enthält zwar eine Rechtsgrundlage für amtliche Publikationen bei kantonalen Angelegenheiten. Für kommunale Abstimmungen und Wahlen fehlt jedoch eine einheitliche Regelung. Auch aus dem Öffentlichkeitsprinzip lässt sich keine Ermächtigung für Internetpublikationen von Personendaten herleiten. Zwar können öffentliche Organe ihrer Informationspflicht auch durch Veröffentlichungen im Internet nachkommen. Die amtliche Informationspflicht umfasst Personendaten jedoch nur sehr beschränkt; so zum Beispiel für eine verhältnismässige Information über Ansprechpartner einer Verwaltungsstelle. Die allgemeine Umschreibung der Pflicht, über Tätigkeiten von öffentlichem Interesse zu informieren, ist keine Ermächtigung für eine Bekanntgabe von Personendaten.

Keine Bekanntgabe von Petitionären

Die Namen von Personen, welche eine Petition unterzeichnen, können durch die Gemeinde nicht bekannt gegeben werden, weil sie Informationen über die politischen Ansichten oder Tätigkeiten sind und deshalb als besondere Personendaten gelten. Betroffene – natürliche und juristische – Personen haben jedoch betreffend ihre eigenen Daten ein Auskunftsrecht.

Eine politische Partei reichte bei der Gemeinde eine Petition ein. Sie verlangte die genaue Prüfung verschiedener Punkte, bevor ein Baubewilligungsverfahren in der Gemeinde überhaupt eingeleitet wird. Die Gemeinde erkundigte sich beim Datenschutzbeauftragten, ob die Namen von Personen, welche die Petition unterzeichnet hatten, bekannt zu geben sind.

Beim Informationszugangsrecht kann jede Person mit schriftlichem Gesuch an die Gemeinde gelangen mit dem Begehren um Einsicht in die Petitionsbögen. Da Personendaten betroffen sind, gelten die Bestimmungen zur Bekanntgabe von Personendaten. Angaben darüber, wer eine Petition unterzeichnet hat, sind besondere Personendaten (Informationen über die politischen Ansichten oder Tätigkeiten). Betrifft das Gesuch besondere Personendaten, lehnt das öffentliche Organ das Gesuch ab, wenn die betroffenen Dritten dem Zugang nicht ausdrücklich zustimmen. Vor jeder Bekanntgabe von Informationen ist auch bei Einwilligung der betroffenen Personen zu beachten, dass im Einzelfall aus Gründen entgegenstehender öffentlicher oder privater Interessen Einschränkungen vorzunehmen sind. Bei dieser Interessenabwägung fällt ins Gewicht, dass es sich bei der politischen Willensäusserung um besondere Personendaten handelt. Die Beantwortung eines Informationszugangsgesuchs erfordert, falls der Zugang zur gewünschten Information verweigert, eingeschränkt oder aufgeschoben werden soll, den Erlass einer Verfügung durch die Gemeinde.

Beim Auskunftsrecht können sämtliche betroffenen Personen – die Petitionäre als natürliche Personen sowie der Verein, der das Baugesuch einreichen will, und die politische Partei als juristische Personen – Zugang zu ihren eigenen Personendaten verlangen. Dabei sind alle Namen der Petitionäre sowohl für den Verein als auch für die Partei eigene Personendaten. Für einen Petitionär hingegen besteht lediglich ein Auskunftsrecht über seine eigenen Angaben auf dem Petitionsbogen. Vor jeder Bekanntgabe ist auch hier zu beachten, dass im Einzelfall aus Gründen entgegenstehender öffentlicher oder privater Interessen Einschränkungen vorzunehmen sind, wobei auch bei dieser Interessenabwägung ins Gewicht fällt, dass die politische Willensäusserung ein besonderes Personendatum ist. Die Petitionäre haben ein gewichtiges privates Interesse daran, dass die Bekanntgabe ihrer Namen unterbleibt. Die Wahrung des Stimmgeheimnisses steht aber auch im öffentlichen Interesse. Gelangt die Gemeinde zum Ergebnis, dass sie das Auskunftsgesuch bezüglich der Bekanntgabe der Namen der Petitionäre verweigern, einschränken oder aufschieben will, hat sie eine entsprechende Verfügung zu erlassen.

Einsatz von Parkplatzdetektiven

Gemeinden sind gestützt auf die Strassenverkehrsgesetzgebung befugt, eine eigene Verordnung für das regelmässige nächtliche Abstellen von Fahrzeugen zu erlassen. Für die Nutzung des öffentlichen Grundes dürfen Gebühren erhoben und betroffene Fahrzeughalter können einer Meldepflicht unterstellt werden. Gemeinden dürfen Dritte mit den dazu notwendigen Überwachungsaufgaben beauftragen.

§ 8 Abs. 1 IDG
Art. 37 Abs. 2 SVG
Art. 20 Abs. 2 VRV

Eine Gemeinde teilte einem nicht ortsansässigen Fahrzeughalter mit, dass eine von ihr beauftragte Firma sein Fahrzeug schon mindestens dreimal in der Nachtparkkontrolle erfasst habe. Dem Fahrzeughalter wurde weiter mitgeteilt, dass regelmässiges nächtliches Dauerparkieren auf öffentlichem Grund gebührenpflichtig sei, sofern er über keine private Abstellmöglichkeit verfüge. Die Gemeinde legte dem Schreiben einen entsprechenden Auszug ihrer Verordnung über das nächtliche Dauerparkieren auf öffentlichem Grund bei.

Weil die betroffene Person mit dieser Überwachungstätigkeit der Gemeinde nicht einverstanden war und auch fürchtete, dass solche Mahnschreiben der Gemeinden in falsche Hände geraten könnten, wandte sie sich an den Datenschutzbeauftragten.

Die Gemeinde hat gestützt auf die Strassenverkehrsgesetzgebung und die dazu gehörige Verkehrsregelnverordnung des Bundes eine eigene Gemeindeverordnung über das nächtliche Dauerparkieren erlassen. Die Gemeindeverordnung schreibt vor, dass es nur mit behördlicher Bewilligung gestattet ist, Fahrzeuge nachts regelmässig auf öffentlichem Grund zu parkieren. Gebührenpflichtig ist, wer sich nicht darüber ausweisen kann, dass ihm ein ausübbares Recht zusteht, sein Fahrzeug über Nacht auf privatem Grund zu parkieren. Gebührenpflichtige Personen haben sich innert 30 Tagen bei der Gemeindeverwaltung zu melden. Zuwiderhandlungen werden mit Busse bestraft. Die Gemeinde verfügt somit über eine rechtliche Grundlage, um Gebühren für nächtliches Dauerparkieren zu erheben.

Der Datenschutzbeauftragte stellte zudem fest, dass es zur Überprüfung, ob betroffene Fahrzeughalter ihrer Meldepflicht nachgekommen sind, notwendig ist, dass die nachts auf öffentlichem Grund abgestellten Fahrzeuge kontrolliert und registriert werden können. Die Gemeinde ist grundsätzlich ermächtigt, diese Aufgabe Dritten zu übertragen. Damit sichergestellt werden kann, dass die gesetzlichen Vorschriften eingehalten werden, erscheint es auch als geeignet und erforderlich, dass die Gemeinde betroffene Fahrzeughalter mit einem Schreiben über ihre Gebührenpflicht in Kenntnis setzt.

Der Datenschutzbeauftragte informierte die betroffene Person, dass das Vorgehen der Gemeinde rechtmässig sei.

Zugang zu Gemeindearchiven

Die Gemeinden haben Akten zu archivieren, die aus einem wissenschaftlichen oder historischen Interesse dauernd aufzubewahren sind. Die Akten müssen sowohl während der Aufbewahrung als auch während der Archivierung vor unberechtigtem Zugriff geschützt werden. Es liegt im Ermessen der Gemeinden, ob sie diese Vorgabe mit einer Zutrittsregelung zu den Archivräumen oder mit separat abschliessbaren Aktenschränken pro Behörde gewährleisten.

§ 5 Abs. 2 IDG
§ 6 Abs. 1 Archivgesetz
§ 6 Abs. 1 Archivverordnung
§ 5 Abs. 3 IDG
§ 8 Abs. 1 IDG
§ 7 Abs. 2 IDG
§ 9 Archivverordnung

Ein Bezirksrat informierte den Datenschutzbeauftragten, dass einige Gemeinden die Akten der Behörden, wie Gemeinderat oder Schulpflege, in *einem* Raum archivieren; Besuchende hätten ungehinderten Zutritt. Der Bezirksrat war der Ansicht, die Gemeinden müssten entweder für abschliessbare Archivschränke oder für separate Archivräume pro Behörde sorgen; eine Zutrittsregelung reiche nicht aus. Um den Gemeinden keinen unrechtmässigen Aufwand zu verursachen, fragte der Bezirksrat den Datenschutzbeauftragten, wie die Archivierung aus datenschutzrechtlicher Sicht korrekt zu erfolgen habe.

Der Datenschutzbeauftragte wies darauf hin, dass zwischen der Aufbewahrung und der Archivierung von Akten unterschieden werden muss: Solange eine Gemeindebehörde Akten für ihre Arbeit regelmässig benötigt, bewahrt sie diese bei sich selbst und nicht im Archiv auf. Werden die Akten nicht mehr benötigt, weil ein Fall – beispielsweise infolge Wegzugs eines Klienten – abgeschlossen wurde, müssen noch die Rechtsmittel- oder Verjährungsfristen abgewartet werden. Bestehen keine solchen Fristen, können Akten noch maximal zehn Jahre seit Abschluss aufbewahrt werden. Nach Ablauf dieser Frist – Fallbearbeitung zuzüglich allfälliger Rechtsmittel- und Verjährungsfristen oder maximal zehn Jahre – bietet die Gemeindbehörde die Akten dem zuständigen Archiv an. Gemeinden führen eigene Archive für ihre Akten. Der Archivverantwortliche der Gemeinde entscheidet, ob Akten beispielsweise wegen eines wissenschaftlichen oder historischen Interesses zu archivieren sind. Beurteilt der Archivverantwortliche Akten als nicht archivwürdig, hat sie die zuständige Gemeindebehörde zu vernichten. Ins Archiv gehören somit ausschliesslich jene Akten, die aus den genannten Gründen dauerhaft aufbewahrt werden.

Unabhängig davon, ob Akten aufbewahrt oder archiviert werden, ist der Zugriff darauf nur jenen Angestellten der Gemeinde zu gewähren, die sie für ihre Aufgaben tatsächlich benötigen. Die Gemeinde hat die angemessenen organisatorischen und technischen Massnahmen zum Schutz vor unbefugtem Zugriff auf Akten zu treffen. Zumindest die Archivräume müssen abschliessbar sein; sonst entscheidet die Gemeinde, wie sie diese Massnahmen umsetzt. Das Gesetz schreibt weder vor, dass ein von mehreren Gemeindebehörden benutzter Archivraum über separat abschliessbare Schränke verfügen muss, noch dass jede Gemeindebehörde einen separaten Archivraum besitzen muss. Bei einem gemeinsamen Archivraum ohne separat abschliessbare Schränke pro Gemeindebehörde darf allerdings nur der Archivverantwortliche ungehinderten Zutritt haben. Er hat Gemeindeangestellten im Einzelfall und auf Gesuch hin Einsicht in archivierte Akten zu geben, wenn diese die Akten für ihre Aufgaben benötigen. Alternativ ist der Zutritt der Gemeindeangestellten in den Archivraum unter Aufsicht des Archivverantwortlichen möglich. Wenn keine dieser beiden oder andere, weniger weit gehende Massnahmen durchführbar sein sollten, sind separat abschliessbare Archivschränke oder für jede Gemeindebehörde separat eingerichtete Archivräume vorzusehen.

Auskunftspflicht gegenüber Sozialversicherung

Die zuständigen Gemeindebehörden müssen Ergänzungsleistungen zur AHV/IV periodisch überprüfen. Massgebend für deren Umfang sind die wirtschaftlichen Verhältnisse der Versicherten. Versicherte sind zur umfassenden Mitwirkung verpflichtet. Um die wirtschaftlichen Verhältnisse abklären zu können, kann die Gemeinde im Einzelfall detaillierte Kontoauszüge einfordern.

Art. 28 Abs. 2 ATSG

Eine Gemeindebehörde forderte im Rahmen der periodischen Überprüfung der Ergänzungsleistungen zur AHV/IV eine versicherte Person auf, detaillierte Bank- und Postkontoauszüge der letzten fünfzehn Monate einzureichen. Die versicherte Person wandte sich an den Datenschutzbeauftragten mit dem Anliegen, die Zulässigkeit dieser Aufforderung zu beurteilen.

Ein gesetzlicher Anspruch auf Ergänzungsleistungen ist gegeben, wenn die Renten und das Einkommen die minimalen Lebenskosten nicht decken. Massgebend sind die wirtschaftlichen Verhältnisse der Versicherten. Diese werden sowohl beim erstmaligen Gesuch als auch im Rahmen der gesetzlich vorgesehenen periodischen Überprüfung ermittelt. Die Versicherten sind bei der Abklärung ihrer wirtschaftlichen Verhältnisse zur Mitwirkung verpflichtet: Sie müssen alle Auskünfte erteilen, die für die Festsetzung der Versicherungsleistung erforderlich sind. Auch haben sie wesentliche Veränderungen ihrer wirtschaftlichen Verhältnisse unaufgefordert zu melden. Wird diese Mitwirkungspflicht missachtet, können Ergänzungsleistungen verweigert oder gekürzt werden.

Angesichts dieser rechtlichen Vorgaben ist grundsätzlich von einer umfassenden Auskunfts- und Meldepflicht der Versicherten auszugehen. Häufig geben nicht nur die Einnahmen, sondern auch die Ausgaben von Versicherten Aufschluss über deren wirtschaftliche Verhältnisse. So können beispielsweise hohe Ausgabebeträge auf nicht deklarierte Einkünfte hinweisen. Auszüge von Bank- und Postkonten der Versicherten sind grundsätzlich geeignet, deren Ein- und Ausgaben zu belegen. Der zuständigen Gemeindebehörde kommt ein gewisses Ermessen zu, in welchem Detaillierungsgrad und über welchen Zeitraum sie Kontoauszüge von Versicherten einverlangt.

Dass die zuständige Behörde detaillierte Kontoauszüge über die vergangenen fünfzehn Monate von der versicherten Person eingefordert hatte, um die wirtschaftlichen Verhältnisse – und letztlich den Anspruch auf den weiteren Bezug von Ergänzungsleistungen – zu ermitteln, erachtete der Datenschutzbeauftragte deshalb als verhältnismässig.

Meldung von sozialhilfeabhängigen Ausländern

Das Bundesrecht verpflichtet die Sozialhilfebehörden, sozialhilfeabhängige Ausländer der kantonalen Migrationsbehörde zu melden. Das Migrationsamt benötigt diese und weitere Informationen, um ausländerrechtliche Massnahmen prüfen zu können. Die systematische Meldung der notwendigen Daten der Sozialhilfebehörden an das Migrationsamt und das Verfahren sind konkret geregelt worden.

Art. 82 Abs. 5 VZAE
Art. 97 Abs. 3 AuG
Art. 82 Abs. 5 VZAE
Art. 63 As. 1 lit. c und
Art. 62 lit. 3 AuG
§ 48 a SHG

Unter Leitung des kantonalen Migrationsamtes entwarf eine Arbeitsgruppe ein Meldeverfahren, das die in der Bundesverordnung über Zulassung, Aufenthalt und Erwerbstätigkeit statuierte Meldepflicht der Sozialhilfebehörden konkretisieren sollte. Die bundesrechtliche Meldepflicht sieht vor, dass ausländische Sozialhilfebezüger unaufgefordert der Migrationsbehörde gemeldet werden müssen.

Im Meldeformular sollten die geeigneten und notwendigen Informationen für die Aufgabenerfüllung des Migrationsamtes festgehalten werden. Dabei galt es abzuwägen, ob beispielsweise auch Höhe und Bezugsdauer der Sozialhilfe Bestandteil der Meldung sein sollten. Denn das Migrationsamt ist im Rahmen seiner Ermessensausübung verpflichtet, die Gründe für den Sozialhilfebezug, die Höhe und Bezugsdauer der Gelder bestimmen, zu berücksichtigen.

Das Migrationsamt legte den Entwurf zum Meldeverfahren dem Datenschutzbeauftragten zur Beurteilung vor. Im Bundesrecht ist nicht genau festgelegt, welche Daten der Meldepflicht unterstehen. Beim Heranziehen weiterer ausländerrechtlicher Bestimmungen muss die unaufgeforderte Meldung deshalb nicht nur den Bezug, sondern auch den Beginn, die Beendigung und den Umfang des Bezugs beinhalten.

Die Arbeitsgruppe legte deshalb im Einzelnen fest, wie die Faktoren, die sich auf die Höhe der Unterstützungsleistung auswirken, im Formular berücksichtigt werden sollen. Das Migrationsamt benötigt zusätzlich zu Umfang und Dauer des Sozialhilfebezugs in jedem Einzelfall weitere Informationen. Die Gründe, die zu den Bezügen geführt haben, sind wesentlich für den ausländerrechtlichen Entscheid. Die Migrationsbehörde hat jeden Einzelfall sorgfältig zu prüfen und den Grundsatz der Verhältnismässigkeit zu wahren.

Mit den Hinweisen zu den Faktoren, die die Sozialhilfebezüge beeinflussen, kann sich in einigen Fällen ein Nachfragen bei der Sozialhilfebehörde erübrigen, oder der ausländerrechtliche Entscheid kann zeitlich aufgeschoben werden. Die systematische Meldung erfolgt erst ab einem gewissen Mindestumfang der Bezüge, was insgesamt eine verhältnismässige Lösung ergibt. Die Regelung, welche Daten künftig bekannt zu geben sind, wurde in das laufende Revisionsverfahren der Sozialhilfegesetzgebung integriert.

Schwarzarbeit ohne Aufenthaltsbewilligung

Personen ohne Aufenthaltsbewilligung, die sich bei der Sozialversicherungsanstalt zur Beitragszahlung anmelden, werden nur an das Migrationsamt weitergemeldet, wenn sie Sozialversicherungsbeiträge nicht geleistet haben und ihr Aufenthalt offensichtlich rechtswidrig ist.

Von Schwarzarbeit wird dann gesprochen, wenn jemand einer Erwerbstätigkeit nachgeht, ohne dafür Sozialversicherungsbeiträge zu bezahlen. Es handelt sich um Beiträge für die Alters- und Hinterbliebenenversicherung, die Invalidenversicherung, die Arbeitslosenversicherung und so weiter. Um Schwarzarbeit effektiver bekämpfen zu können, wurde das Bundesgesetz gegen Schwarzarbeit erlassen und am 1. Januar 2008 in Kraft gesetzt. Unter anderem wurden administrative Erleichterungen durch ein vereinfachtes Abrechnungsverfahren bei den Sozialversicherungen für kleinere unselbständige Tätigkeiten, beispielsweise für Haushaltshilfen, geschaffen.

Eine Arbeitgeberin wollte für ihre Haushaltshilfe, die keine gültige Aufenthaltsbewilligung besitzt, die gesetzlich vorgeschriebenen Sozialversicherungsbeiträge entrichten. Die Arbeitgeberin befürchtete, die Sozialversicherungsanstalt könnte die Information, dass sich die Hausangestellte nicht rechtmässig in der Schweiz aufhält, an die Migrationsbehörde weitermelden, was zu deren Ausschaffung führen könnte. Dem Datenschutzbeauftragten wurde die Frage vorgelegt, ob hier eine Anzeige an das Migrationsamt ausgeschlossen sei.

Der Datenschutzbeauftragte prüfte die Rechtslage und nahm Rücksprache mit der Sozialversicherungsanstalt. Das Gesetz gegen die Schwarzarbeit sieht vor, dass die für den Vollzug der Sozialversicherungsgesetzgebung zuständigen kantonalen Behörden, zu welchen auch die Sozialversicherungsanstalt gehört, Ergebnisse ihrer Kontrollen dem Migrationsamt bekannt geben, wenn die folgenden beiden Voraussetzungen kumulativ erfüllt sind. Erstens hat die betroffene Person aus unselbständiger oder selbständiger Erwerbstätigkeit ein Einkommen erzielt, für welches die Sozialversicherungsbeiträge nicht entrichtet wurden. Zweitens hat sich sogleich ergeben, dass der Aufenthalt der betroffenen Person mit den geltenden Bestimmungen nicht übereinstimmt.

Das Gesetz regelt damit, in welchen Fällen Informationen über Personen ohne Aufenthaltsbewilligung an das Migrationsamt zu erfolgen haben, nämlich wenn Schwarzarbeit vorliegt. Umgekehrt gilt aber auch, dass Personen ohne Aufenthaltsbewilligung, welche sich bei der Sozialversicherungsanstalt zur Beitragszahlung anmelden, nicht an Asyl- und Ausländerbehörden weitergemeldet werden dürfen. Dies konnte der Arbeitgeberin vom Datenschutzbeauftragten – übereinstimmend mit der Haltung der Sozialversicherungsanstalt – versichert werden.

IDG gilt bei hängigen Strafverfahren

Das IDG ist im Gegensatz zum früheren Datenschutzgesetz auch auf hängige Strafverfahren anwendbar. Der Anspruch auf Informationszugang richtet sich indessen in nicht rechtskräftig abgeschlossenen Verfahren nach der Strafprozessordnung. Das Auskunftsrecht in Bezug auf eigene Daten kann nach datenschutzrechtlichen und verfahrensrechtlichen Bestimmungen geltend gemacht werden.

§ 3 Abs. 2 lit. b aDSG ZH
§ 2 Abs. 1 IDG
§ 20 IDG

Das frühere Datenschutzgesetz galt ausdrücklich nicht für die hängigen Verfahren der Strafrechtspflege. Der Geltungsbereich des IDG ist neu auf Instanzen ausgerichtet: Die Gerichte sind explizit ausgeschlossen. Im Zusammenhang mit dem Recht auf Informationszugang stellte sich die Frage, ob während eines hängigen Strafverfahrens IDG und Strafprozessordnung (StPO) parallel anwendbar sind. Dabei geht es um die Auslegung von § 20 Abs. 3 IDG.

Im Verlaufe der Beratungen des IDG wurden die Gerichte vom Geltungsbereich des IDG ausgenommen. Dies wurde damit begründet, dass mit der Akteneinsichtsverordnung der obersten Gerichte bereits eine ausführliche Regelung für die Informationszugangsrechte sowohl für Dritte als auch für andere Gerichte und Behörden existierte. Deshalb seien Verfahren vor Gericht, nicht aber Verfahren der Strafuntersuchungsbehörden bis zur Anklageerhebung, vom Geltungsbereich des IDG auszunehmen.

Das Recht auf Zugang zu Informationen richtet sich in nicht rechtskräftig abgeschlossenen Verwaltungs- und Verwaltungsjustizverfahren nach dem massgeblichen Verfahrensrecht. Streng genommen können die von den Strafverfolgungsbehörden vorgenommenen Handlungen nicht den Verwaltungs- und Verwaltungsjustizverfahren zugeordnet werden. Dass diese Verfahren im Gesetz nicht erwähnt sind, deutet jedoch auf ein redaktionelles Versehen hin, war doch in der Weisung zum IDG noch explizit die Strafprozessordnung als Beispiel für ein mögliches anwendbares Verfahrensrecht genannt.

Die Oberstaatsanwaltschaft und der Datenschutzbeauftragte kamen nach einer gemeinsamen Auslegeordnung zum Schluss, dass das IDG generell auch auf Strafverfahren anwendbar ist. Für Gesuche um Informationszugang gilt in hängigen Strafverfahren sinngemäss § 20 Abs. 3 IDG. Demnach sind die Bestimmungen der StPO anwendbar. Die Weisungen der Oberstaatsanwaltschaft zur Untersuchungsführung wurden entsprechend angepasst.

Unberührt von dieser Regelung bleibt der Zugang zu den eigenen Personendaten. Dieses Auskunftsrecht kann immer gestützt auf den datenschutzrechtlichen oder den verfahrensrechtlichen Anspruch geltend gemacht werden.

Löschung von Daten im Strafverfahren

Die Staatsanwaltschaft entscheidet, welche Daten zur Beweisführung beschlagnahmt und spätestens nach Abschluss der Untersuchung gelöscht werden. Der datenschutzrechtliche Anspruch auf Löschung kann durch die betroffene Person direkt bei der zuständigen Staatsanwaltschaft geltend gemacht werden.

§§ 88 ff. und 96 ff. StPO
§ 72 a Gerichtsverfassungsgesetz
§ 17 StPO
§ 98 i.V.m. § 106 StPO

In einem Ermittlungsverfahren wegen Brandstiftung beschlagnahmte die Kantonspolizei im Auftrag der Staatsanwaltschaft bei einer Hausdurchsuchung Computer und externe Festplatten. Auf den Datenträgern befanden sich sowohl private Daten als auch Daten der Firma des Angeschuldigten. Die Staatsanwaltschaft spiegelte sämtliche Daten und gab die Datenträger sodann dem Angeschuldigten zurück.

Der Angeschuldigte beschwerte sich beim Datenschutzbeauftragten: Die Daten seien willkürlich beschlagnahmt worden und für die Ermittlungen nicht relevant. Er bat den Datenschutzbeauftragten um Unterstützung, damit die Daten sofort gelöscht werden.

Die in einem Strafverfahren beschlagnahmten Personendaten sind besondere Personendaten, deren Bearbeitung einer hinreichend bestimmten Regelung in einem formellen Gesetz bedürfen. Gesetzliche Bestimmungen für eine Hausdurchsuchung und die Beschlagnahme von Gegenständen sowie für die Akteneinsicht in einer laufenden Strafuntersuchung finden sich in der Strafprozessordnung. Parallel dazu kann die betroffene Person ein Gesuch auf Zugang zu den eigenen Personendaten stellen und weitere datenschutzrechtliche Ansprüche geltend machen. Wird dem Begehren mittels beschwerdefähiger Verfügung nicht entsprochen, kann der Entscheid auf verwaltungsrechtlichem Weg angefochten werden.

Im Rahmen einer Deliktklärung prüft die zuständige Staatsanwaltschaft, welche Daten für die Beweissicherung benötigt werden. Sie entscheidet im konkreten Fall – unter Beachtung des Verhältnismässigkeitsprinzips und spätestens nach Abschluss der Strafuntersuchung –, welche von den erhobenen Personendaten zu löschen sind.

Der Datenschutzbeauftragte empfahl dem Angeschuldigten, seinen Anspruch auf Löschung der gespiegelten Daten direkt bei der zuständigen Staatsanwaltschaft geltend zu machen.

DNA-Profile Minderjähriger

Für DNA-Profile von jugendlichen Straftätern gelten dieselben Aufbewahrungs- und Löschfristen wie für Erwachsene. Im Einzelfall kann dies unverhältnismässig sein. Mit der geplanten Inkraftsetzung der neuen Jugendstrafprozessordnung wird diesem Umstand Rechnung getragen: Das DNA-Profil-Gesetz wird um Löschfristen erweitert, die spezifisch auf die Massnahmen und Sanktionen des Jugendstrafrechts ausgerichtet sind.

Der Datenschutzbeauftragte wurde angefragt, ob es verhältnismässig sei, dass das DNA-Profil eines Jugendlichen fünf Jahre und die Fingerabdrücke zwanzig Jahre lang gespeichert bleiben oder ob es Möglichkeiten gibt, dass diese Personendaten früher gelöscht werden können.

Auch die Aufbewahrungs- und Löschfristen unterliegen dem Verhältnismässigkeitsprinzip. Dass für die DNA-Profile von Jugendlichen die gleichen Aufbewahrungs- und Löschfristen wie für erwachsene Straftäter gelten, kann im Einzelfall unverhältnismässig sein. Wie auch bei der Anordnung der erkennungsdienstlichen Massnahmen soll bei der Interessenabwägung zwischen Strafverfolgung und Eingriff nicht nur das Interesse der Strafverfolgung einbezogen werden, sondern auch das jugendliche Alter und die Schwere des Delikts. Wenn es sich um ein erstmaliges Delikt handelt und kein weiterer Verdacht vorliegt, ist es fraglich, inwiefern die gespeicherten Daten zur Aufklärung weiterer Delikte geeignet und erforderlich sind. Allerdings lässt sich erst nach Ablauf einer gewissen Zeitspanne beurteilen, ob sich die betroffene Person Weiteres zuschulden kommen lässt.

Das IDG bietet in diesen Fällen die Möglichkeit, Rechtsansprüche wie die vorzeitige Löschung geltend zu machen. Der Ablehnungsentscheid durch das öffentliche Organ kann auf verwaltungsrechtlichem Weg angefochten werden. Zu berücksichtigen ist dabei die Meinung des Bundesgerichts, welches Erhebung und Aufbewahrung von erkennungsdienstlichem Material als leichten Eingriff in die persönliche Freiheit qualifiziert. Die Schweizerische Jugendstrafprozessordnung, die voraussichtlich 2011 in Kraft treten wird, trägt diesen Umständen Rechnung: Das DNA-Profil-Gesetz wird, falls Sanktionen nach dem Jugendstrafgesetz ausgesprochen werden, angepasste Löschfristen für diese DNA-Profile enthalten.

Polizei überprüft Hotelgäste

Hotels müssen eine Gästekontrolle führen und diese Informationen der Polizei zur Verfügung stellen. Betroffen davon sind auch schweizerische Staatsangehörige, obwohl das europäische und das Bundesrecht nur ein Meldeverfahren für ausländische Staatsangehörige verlangen. Zudem werden alle Daten mit dem Schengener Informationssystem abgeglichen. Die faktische Ausweispflicht für schweizerische Staatsangehörige und die elektronische Fahndungsabfrage erfordern eine noch zu schaffende Rechtsgrundlage.

§ 32 Abs. 3 GG

Beherbergungsbetriebe sind verpflichtet, über ihre Gäste Buch zu führen. Die verwendeten Meldescheine müssen anschliessend der Polizei zur Verfügung gestellt werden. Seit 2009 werden die Meldescheine elektronisch bearbeitet. Zusätzlich werden die Meldescheine nicht nur mit dem Fahndungssystem Ripol abgeglichen, sondern auch mit dem Schengener Informationssystem (SIS).

Der Datenschutzbeauftragte hielt in einer Stellungnahme fest, dass die Rechtsgrundlage im Hinblick auf die elektronische Bearbeitung zu überprüfen ist. Sowohl die eidgenössische Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit als auch das Schengener Durchführungsübereinkommen sehen nur ein Meldeverfahren der Beherbergungsbetriebe für ausländische Staatsangehörige vor; das Gemeindegesetz, das die Gästekontrolle regelt, unterscheidet nicht zwischen schweizerischen und ausländischen Staatsangehörigen. Zusätzlich besteht für den erweiterten Abgleich der Informationen durch die Polizei mit dem SIS keine Rechtsgrundlage. Die automatisierte, systematische und verdachtsunabhängige Kontrolle ist eine Bearbeitung von besonderen Personendaten und bedarf einer formellgesetzlichen Grundlage entweder im Gemeinde- oder in einem anderen Gesetz.

Der Datenschutzbeauftragte hat im Rahmen der Vernehmlassung zur Revision des Gemeindegesetzes darauf hingewiesen. Aufgrund seiner Intervention hat auch die Kantonspolizei diesen Einwand entgegengenommen und wird das Anliegen mit der Sicherheitsdirektion behandeln. Der Regierungsrat hält in der Antwort auf das dringliche Postulat «Datenschutz für Schweizer Hotelgäste» (KR-Nr.381/2009) fest, dass die Sicherheitsdirektion Änderungen der Polizeigesetzgebung prüfe und dass die Frage der Hotelkontrolle ein Teil dieser Prüfung sei.

Harmonisierung der Einwohnerregister

Die Umsetzung des Registerharmonisierungsgesetzes muss gewährleisten, dass Daten, die zu statistischen Zwecken erhoben werden, nicht anderweitig verwendet werden. Auch die Ersterfassung der Grunddaten durch eine Drittfirma muss ausschliessen, dass diese Firma die Daten zu eigenen Zwecken nutzen kann. Eine künftige Verwendung der Sozialversicherungsnummer in den Registern braucht eine bereichsspezifische Regelung.

Das Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (Registerharmonisierungsgesetz) wurde im Hinblick auf die registergestützte Volkszählung erlassen und hatte Anpassungen des Gemeindegesetzes zur Folge. Der Datenschutzbeauftragte nahm hierzu im Rahmen der Vernehmlassung und in der parlamentarischen Kommission Stellung.

Neu haben die Einwohnerkontrollen auch Personendaten zu bearbeiten, die nur für statistische Zwecke erhoben werden. Hierzu gehören beispielsweise auch Angaben über Insassen in Strafvollzugsanstalten und Klienten in psychiatrischen Einrichtungen. Solche Daten dürfen nicht – im Gegensatz zu Angaben über die Einwohnerinnen und Einwohner einer Gemeinde – an private Personen weitergegeben werden. Die unterschiedliche Verwendungsmöglichkeit dieser Daten musste deshalb klar geregelt werden. Der Datenschutzbeauftragte schlug vor, in einzelnen Paragrafen zu verdeutlichen, dass bestimmte Angaben nur zu statistischen Zwecken Verwendung finden dürfen und nur die jeweiligen Statistikverantwortlichen Zugriff auf diese Daten erhalten. Des Weiteren konnte auf die problematische Lösung der Gästekontrolle im Rahmen des Gemeindegesetzes hingewiesen werden (siehe Seite 45).

Im Rahmen der parlamentarischen Beratung kam zur Sprache, dass eine Drittfirma, die Post, die Gebäude- und Wohnungsnummern erstmals erfassen und den Personen zuordnen soll. Die Post hatte sich schon früher an die Datenschutzbeauftragten der Kantone Basel-Stadt und Zürich gewandt, um mit ihnen die datenschutzrechtlichen Rahmenbedingungen eines solchen Vorhabens zu besprechen. Obwohl die Post ein grosses Eigeninteresse hat, ihre Daten in diesem Zusammenhang auch zu aktualisieren, ist dies rechtlich ausgeschlossen. Die involvierten öffentlichen Organe dürfen die Post für die erwähnten Tätigkeiten beauftragen; es muss indessen organisatorisch und technisch verhindert werden, dass die Daten, die von der Post erhoben werden, auch von der Post verwendet werden können. Dies ist entsprechend in einem Vertrag mit der Post festzulegen. Der vorgelegte Mustervertrag war in einzelnen Punkten anzupassen, und das Statistische Amt versicherte, dass es den Vertrag vor Abschluss nochmals dem Datenschutzbeauftragten zur Prüfung vorlegen würde.

Im Rahmen der Führung verschiedener Register stellt sich auch die Frage, wie weit die neue Sozialversicherungsnummer Verwendung finden kann. Das Bundesrecht ermöglicht es den Kantonen, die Sozialversicherungsnummer auch unter bestimmten Voraussetzungen für Verwaltungszwecke zu nutzen. Der Datenschutzbeauftragte beurteilte einen ersten Regelungsvorschlag auf kantonaler Ebene. Dabei wurde festgehalten, dass eine Pauschalermächtigung zur Verwendung der Sozialversicherungsnummer keinen Rückhalt im Bundesrecht findet. Vielmehr ist analog der Regelung auf Bundesebene bereichsspezifisch zu prüfen, wo die Verwendung der Sozialversicherungsnummer geeignet und erforderlich ist. Dabei ist sicherzustellen, dass die Nummer nur für die bereichsspezifischen Zwecke verwendet wird. Eine entsprechende gesetzliche Grundlage ist noch nicht geschaffen worden.

Logdaten für Arbeitszeitkontrolle

Elektronische Schliesssysteme zeichnen die gewährten und verweigerten Zutritte samt Zeitpunkt und verwendeten elektronischen Schlüsseln auf. Anhand der Logdaten ist ersichtlich, wann Mitarbeitende Büroräumlichkeiten betreten oder verlassen haben. Die Logdaten dürfen nur für die Überprüfung der Arbeitszeiteintragungen von Mitarbeitenden verwendet werden, wenn eine rechtliche Bestimmung diesen Zweck ausdrücklich vorsieht oder die Einwilligung der betroffenen Personen vorliegt.

Amtsstellen, die elektronische Schliesssysteme für ihre Büroräumlichkeiten verwenden, zeichnen für die technische Überwachung die gewährten und verweigerten Zutritte sowie den Zeitpunkt und die verwendeten elektronischen Schlüssel als Logdaten auf. Aus den Logdaten ist ersichtlich, wann Mitarbeitende die Büroräumlichkeiten betreten oder verlassen haben. Der Datenschutzbeauftragte wurde von einer Amtsstelle angefragt, ob diese Logdaten verwendet werden dürfen, um zu überprüfen, ob einzelne Mitarbeitende ihre Arbeitszeiten richtig eingetragen haben.

Das öffentliche Organ darf Personendaten nur zu dem Zweck bearbeiten, zu dem sie erhoben wurden, soweit nicht eine rechtliche Bestimmung ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt. Die Logdaten der elektronischen Schliesssysteme umfassen Datum, Zeit und die einmalige Identitätsnummer des Schliesssystemanbieters. Anhand der Identitätsnummer können die Daten einer Person zugeordnet werden. Die Bewegungen an den elektronischen Türen werden aus Sicherheitsaspekten und zum Nachvollziehen strafrechtlich relevanter Vorkommnisse wie Beschädigung oder Diebstahl gespeichert. Das Speichern bezweckt nicht die Kontrolle der Anwesenheiten der Mitarbeitenden, sondern dient der Personen- und Gebäudesicherheit. Eine personalrechtliche Bestimmung zur Verwendung der Logdaten für die Arbeitszeitkontrolle besteht nicht, weil diese Verwendung nicht vorgesehen ist. Die Angestellten haben vielmehr auf Vertrauensbasis eine persönliche Arbeitszeitbuchhaltung zu führen. Diese Zweckbindung erlaubt nicht, dass die Logdaten verwendet werden, um die Arbeitszeiten der Mitarbeitenden zu überprüfen.

Die Logdatenverwendung kann notwendig sein, wenn Mitarbeitende ihre Arbeitspflichten nicht erfüllen und ein Verdacht besteht, dass der Grund in nicht erfassten Abwesenheiten liegt. Kann dies nicht anders überprüft werden, ist eine Logdatenverwendung notwendig. Die Schliesssystemdaten sind jedoch für die Arbeitszeitkontrolle nur bedingt geeignet. Betritt ein Mitarbeiter zusammen mit anderen das Gebäude und wird nur ein Schlüssel benützt, sind die Daten nicht vollständig und somit nicht geeignet. Sind die Logdaten für die Überprüfung der Arbeitszeit zu verwenden, ist den Mitarbeitenden vorzuschreiben, das Betreten und Verlassen des Gebäudes nur mit Badge vorzunehmen. Liegen Hinweise für gefälschte Zeitbuchhaltungen vor, ist Strafanzeige wegen Betrugs einzureichen. Im Strafverfahren können die Logdaten gestützt auf strafprozessrechtliche Bestimmungen bearbeitet und bekannt gegeben werden.

Der Datenschutzbeauftragte regte an, Logdaten von Zutrittssystemen künftig so auszugestalten, dass ein Personenbezug bei Randdaten vermieden wird. Werden die Daten nicht gelöscht, sollen sie möglichst bald anonymisiert oder pseudonymisiert werden.

Anmeldung zum Bezug von Familienzulagen

Der Arbeitnehmer kann das Anmeldeformular zum Bezug von Familienzulagen wahlweise seinem Arbeitgeber oder direkt der Familienausgleichskasse einreichen. Das dafür vorgeschriebene Anmeldeformular und allfällige vom Arbeitnehmer einzureichende Unterlagen haben sich auf jene Angaben zu beschränken, die für die Abklärung des Anspruchs auf Familienzulagen notwendig sind.

Am 1. Januar 2009 trat das Bundesgesetz über die Familienzulagen (FamZG) in Kraft. Die Ausrichtung von Familienzulagen wird neu einheitlich vom Bund geregelt. Die Umsetzung ist im Kanton Zürich im Einführungsgesetz zum FamZG geregelt. Bisher sah die Anmeldung zum Bezug von Familienzulagen über die Sozialversicherungsanstalt des Kantons Zürich (SVA) vor, dass das dafür vorgeschriebene Anmeldeformular zunächst vom Arbeitnehmer auszufüllen, zu unterzeichnen und zusammen mit den erforderlichen Unterlagen (z.B. Familienausweis oder Scheidungsurteil) an den Arbeitgeber weiterzuleiten war. Der Arbeitgeber hatte sodann das Anmeldeformular mit seinen Angaben zu ergänzen und ebenfalls unterzeichnet an die Familienausgleichskasse der SVA weiterzuleiten. Durch diesen Ablauf erhielt der Arbeitgeber Einsicht in Angaben des Arbeitnehmers, die zwar von der Familienausgleichskasse der SVA zur Abklärung des Anspruchs auf Familienzulagen, nicht jedoch vom Arbeitgeber zur Durchführung des Arbeitsverhältnisses benötigt wurden. So erfuhr der Arbeitgeber beispielsweise die Einkommenshöhe des Ehegatten seines Arbeitnehmers oder er konnte Einsicht in das Scheidungsurteil nehmen, wenn der Arbeitnehmer in geschiedener oder gerichtlich getrennter Ehe lebte.

Der Datenschutzbeauftragte wies die SVA darauf hin, dass die Anmeldung zum Bezug von Familienzulagen organisatorisch so ausgestaltet werden müsse, dass der Arbeitgeber keine Einsicht in Angaben des Arbeitnehmers erhalte, die zur Prüfung des Anspruchs auf Familienzulagen erhoben werden. Weiter legte der Datenschutzbeauftragte der SVA dar, dass sie vom Arbeitnehmer nur jene Angaben und Unterlagen verlangen dürfe, die geeignet und erforderlich sind, um seinen Anspruch auf Familienzulagen abzuklären. Für die Festsetzung von Familienzulagen wird beispielsweise nicht das gesamte Scheidungsurteil benötigt, das sehr persönliche Angaben über den Arbeitnehmer, dessen Ex-Ehegatten sowie über dessen Kinder enthalten kann. Als Beleg, welchem Ehegatten die elterliche Sorge zusteht, genügt ein entsprechender Auszug aus dem Scheidungsurteil. Aus diesen Gründen ersuchte der Datenschutzbeauftragte die SVA, das von ihr zum Bezug von Familienzulagen angewendete Anmeldeverfahren sowie das dafür vorgeschriebene Formular entsprechend anzupassen.

Die SVA hat den Handlungsbedarf erkannt und das Anmeldeverfahren und -formular angepasst. Die Angaben durch den Arbeitgeber wurden an den Anfang des Formulars gestellt. Auf dem Formular ist zudem die Möglichkeit vermerkt, dass der Arbeitnehmer dieses – versehen mit den Angaben des Arbeitgebers – direkt an die SVA senden kann. Bei geschiedenen Eltern wird als Beleg für die elterliche Sorge nun lediglich eine Kopie der ersten Seite und der entsprechenden Passage aus dem Scheidungsurteil verlangt. Schliesslich verlangt die SVA statt der Angabe des Einkommens des Ehegatten nur noch, ob dieses höher oder tiefer ist als dasjenige des Antragstellers.

Deaktivierung von E-Mail-Adressen

Nach dem Austritt von Mitarbeitenden sind E-Mail-Adressen zu deaktivieren. Bevor sie endgültig gelöscht werden, sind unter Umständen noch geschäftliche Informationen sicherzustellen. Falls betreffende Mitarbeitende nicht mehr in der Lage oder bereit sind, dies selbständig zu erledigen, kann eine Ersatzvornahme erfolgen. Diese hat verhältnismässig zu sein.

§ 11 Abs. 2 IDG
§ 7 Abs. 2 lit. b IDG

Der Datenschutzbeauftragte wird immer wieder angefragt, wie mit E-Mail-Adressen von Mitarbeitenden zu verfahren sei, die den Arbeitsplatz für längere Zeit oder definitiv verlassen. So gelangte eine ehemalige Mitarbeiterin eines öffentlichen Organs mit der Bitte an den Datenschutzbeauftragten, ihre E-Mail-Adresse bei ihrem ehemaligen Arbeitgeber löschen zu lassen. Das öffentliche Organ führte ihre E-Mail-Adresse auch Monate nach ihrem Austritt als Kontaktadresse auf zahlreichen Webseiten auf. Die ehemalige Mitarbeiterin hatte sich mehrmals erfolglos bemüht, dass diese E-Mail-Adresse gelöscht werde.

Die meisten Mitarbeitenden der kantonalen Verwaltung verfügen über eine persönliche E-Mail-Adresse. Sie wird für dienstliche E-Mails verwendet und kann – in beschränktem Umfang – auch für private E-Mails genutzt werden. Das öffentliche Organ, das Informationen über seine Organisation, Zuständigkeiten und Ansprechpersonen zur Verfügung stellt, kann auch E-Mail-Adressen der Mitarbeitenden nach aussen kommunizieren. Diese Informationen müssen stets aktuell und korrekt sein.

Falls Mitarbeitende ihren Arbeitsplatz für längere Zeit oder definitiv verlassen, muss der Arbeitgeber Massnahmen treffen, die dem Datenschutzrecht, dem Personalrecht sowie den Interessen des Arbeitgebers Rechnung tragen. Im genannten Einzelfall konnte der Datenschutzbeauftragte rasch eine einvernehmliche Lösung erwirken: Die E-Mail-Adresse wurde gelöscht. Weil sich diesbezüglich eine generelle Unsicherheit in der Verwaltung abzeichnet, hat der Datenschutzbeauftragte die Erarbeitung entsprechender Arbeitshilfen eingeleitet.

Grundsätzlich sollten E-Mail-Adressen nach dem Austritt der Mitarbeitenden deaktiviert werden. Wenn allfällige geschäftliche E-Mails, die weder durch Kontaktieren der ausgetretenen Mitarbeitenden noch beim Absender beschafft werden können, im gesperrten Konto aber allenfalls noch vorhanden sind, kann nach Androhung und unter Einräumung einer angemessenen Frist eine Ersatzvornahme durch den Arbeitgeber durchgeführt werden. Eine Ersatzvornahme ist ausschliesslich damit begründbar, dass der dringlich anstehende Geschäftsfortgang verhindert wird. Es darf also nur auf E-Mails zugegriffen werden, falls dies zur Erfüllung der gesetzlich umschriebenen Aufgaben notwendig ist. Falls ein solcher Zugriff erfolgen soll, sind betreffende Mitarbeitende vorgängig darauf hinzuweisen und es ist ihnen eine Frist zur selbständigen Erledigung einzuräumen. Zudem hat die Ersatzvornahme verhältnismässig zu sein. Dem kantonalen Personalamt wurden Vorschläge für eine einheitliche Regelung vorgelegt.

Regeln für das Austrittsgespräch

Austrittsgespräche im Personalbereich werden innerhalb der kantonalen Verwaltung einheitlich durchgeführt. Die neue Regelung entspricht bezüglich Verhältnismässigkeit nicht dem IDG, und ein einheitlicher Gesprächsablauf fehlt. Für weiter gehende Auswertungen ist zudem eine gesetzliche Grundlage zu schaffen.

Die Geschäftsprüfungskommission (GPK) setzte sich mit dem Personalcontrolling der Direktionen und des Regierungsrats auseinander. In ihrem Bericht empfahl sie unter anderem, dass die Austrittsgespräche der Mitarbeitenden einheitlich durchgeführt und verbindlich geregelt werden. Der Regierungsrat bestätigte diese Empfehlung, und eine direktionsübergreifende Arbeitsgruppe erarbeitete Dokumente zum Austrittsgespräch und dessen Ablauf. Der Datenschutzbeauftragte wurde zum Mitbericht eingeladen.

Der Datenschutzbeauftragte hielt fest, dass sowohl die Empfehlungen der GPK als auch der Beschluss des Regierungsrates, verbindliche Regelungen für die Durchführung des Austrittsgesprächs zu schaffen, mit den Anforderungen, die das IDG an die hinreichend bestimmte Regelung des Austrittsgesprächs stelle, übereinstimmen. Er begrüsste grundsätzlich die geplante Vereinheitlichung der Austrittsgespräche, wies aber darauf hin, dass nicht ersichtlich sei, ob der Detaillierungsgrad des Fragebogens für das Austrittsgespräch – welchen der Antrag an den Regierungsrat vorsieht – für das Controlling und die Mitarbeitendenzufriedenheit geeignet und erforderlich sei. Weiter hielt er fest, dass der Austrittsablauf im Antrag nicht ausgeführt werde: Es fehlten Angaben darüber, wer am Gespräch teilnehme, ob es eine Auswertung gebe, wer diese gegebenenfalls vornehmen würde und wie die Ergebnisse weiterverwendet würden. Offen sei auch, ob die Fragebogen aufbewahrt oder unmittelbar nach dem Gespräch vernichtet würden. Der Datenschutzbeauftragte forderte entsprechende Präzisierungen.

Sollten mit dem Austrittsgespräch weitere Zwecke oder Auswertungen verbunden sein, die Fragebogen aufbewahrt werden oder Personendaten aufgrund des Auswertungsgesprächs in anderer Weise bearbeitet werden, so sind dafür entsprechende formellgesetzliche Grundlagen zu schaffen. Eine gesetzliche Grundlage müsste die entsprechenden Datenbearbeitungen so regeln, dass diese für alle Beteiligten nachvollziehbar wären.

Der Regierungsrat hat beschlossen, die einheitlichen Regelungen zu den Austrittsgesprächen im Rahmen eines Pilotprojekts für drei Jahre einzuführen (RRB Nr. 1071/2009). Die Anregungen des Datenschutzbeauftragten blieben weitgehend unberücksichtigt. Im Rahmen einer Wegleitung wurden lediglich die Zweckbindung beim auszufüllenden Fragebogen sowie die Vernichtung der Fragebogen minimal und aus datenschutzrechtlicher Sicht ungenügend festgehalten.

Vollmacht für Vertrauensarzt

Pensionskassen entscheiden aufgrund einer vertrauensärztlichen Untersuchung über die Leistung bei Berufs- und Erwerbsinvalidität. Versicherte sind grundsätzlich zu einer vertrauensärztlichen Untersuchung verpflichtet. Die Vollmacht, mit der sie den Vertrauensarzt ermächtigen, Auskünfte einzuholen, muss hinreichend bestimmt sein: Versicherte müssen aus dieser erkennen können, zu welchem Zweck der Vertrauensarzt welche Auskünfte über sie bei Dritten einholt und der Pensionskasse weitergibt.

§ 19 Abs. 2 und § 21 Abs. 2 Statuten der Versicherungskasse für das Staatspersonal
§ 7 Verwaltungsrechtspflegegesetz
Art. 28 ATSG
§ 55 Personalgesetz
Art. 321 StGB
§ 8 Abs. 1 IDG

Die Pensionskasse für Kantonsangestellte forderte einen Versicherten, der seit mehreren Monaten krankheitshalber arbeitsunfähig geschrieben war, auf, sich einer vertrauensärztlichen Untersuchung zu unterziehen. Der Versicherte erhielt dazu von der Pensionskasse ein Vollmachtsformular, mit dem er den Vertrauensarzt ermächtigen sollte, Auskünfte über ihn bei Dritten, wie anderen Ärzten und dem Arbeitgeber, einzuholen. Die Vollmacht enthielt den Hinweis, dass im Weigerungsfalle Versicherungsleistungen gekürzt würden. Der Versicherte reichte diese Vollmacht dem Datenschutzbeauftragten ein und bat ihn zu prüfen, ob sie mit den datenschutzrechtlichen Anforderungen übereinstimme.

Die Pensionskasse entscheidet aufgrund der vertrauensärztlichen Untersuchung über die Leistung bei Berufs- oder Erwerbsinvalidität. Der Vertrauensarzt trifft die nötigen Abklärungen – sowohl bei den Versicherten als auch bei Dritten –, um festzustellen, ob und wie weit eine Invalidität vorliegt. Versicherte sind grundsätzlich verpflichtet, sich einer vertrauensärztlichen Untersuchung zu unterziehen, dem Vertrauensarzt alle für die Abklärung notwendigen Auskünfte zu erteilen und Dritte zur Auskunft zu ermächtigen. Verweigern Versicherte ihre Mitwirkung, kann die Pensionskasse Versicherungsleistungen abweisen oder kürzen.

Der Vertrauensarzt untersteht der Schweigepflicht in Bezug auf Tatsachen, die ihm infolge seines Berufes anvertraut wurden oder die er in dessen Ausübung wahrgenommen hat. Mit der ausdrücklichen Einwilligung der Versicherten wird der Vertrauensarzt von der Schweigepflicht entbunden. Die Vollmacht, mit der Versicherte den Vertrauensarzt ermächtigen, Auskünfte einzuholen, muss sich auf den konkreten Fall beziehen. Die Vollmacht muss nicht nur die Pensionskasse als Empfängerin und den Vertrauensarzt als Absender von Informationen über die Versicherte nennen, sondern auch die gegenüber dem Vertrauensarzt zur Auskunft ermächtigten Dritten. Zudem muss die Vollmacht den Zweck – vertrauensärztliche Untersuchung des Versicherten zur Abklärung des Leistungsanspruchs infolge Krankheit oder Unfall – umschreiben. Gemäss dem Prinzip der Verhältnismässigkeit dürfen nur Auskünfte eingeholt und erteilt werden, die geeignet und erforderlich sind, um den Leistungsanspruch abklären zu können.

Das Vollmachtsformular, das dem Datenschutzbeauftragten von der anfragenden Person vorgelegt wurde, genügte diesen Anforderungen nur teilweise. Nach Intervention des Datenschutzbeauftragten hat die Pensionskasse das Vollmachtsformular zusammen mit weiteren Formularen für die vertrauensärztliche Untersuchung von Versicherten überarbeitet. Die Formulare entsprechen nun den datenschutzrechtlichen Anforderungen.

Mustervertrag für Case-Management

Die Case-Management-Vereinbarungen zwischen öffentlich-rechtlichen Spitälern und Krankenversicherungen sind noch nicht an die gültige Rechtslage angepasst, trotz Intervention des Datenschutzbeauftragten und Kreisschreiben der Gesundheitsdirektion. Der Datenschutzbeauftragte hat deshalb einen Mustervertrag für das Case-Management der Krankenversicherungen angeregt, der nun vom Verband Zürcher Krankenhäuser unter Einbezug aller Beteiligten erarbeitet werden soll.

Verschiedene Krankenversicherungen haben mit öffentlich-rechtlichen Spitälern Vereinbarungen betreffend Case-Management geschlossen. Je nach Krankenversicherung und Spital sind diese Vereinbarungen zwar unterschiedlich ausgestaltet, enthalten aber etwa die gleichen Regelungen. Der Datenschutzbeauftragte hat darauf hingewiesen, dass diese Vereinbarungen häufig rechtswidrig sind (siehe Tätigkeitsbericht Nr. 14 [1.–9.2008], S. 10 f.), was zu politischen Vorstössen sowohl auf Bundesebene als auch in anderen Kantonen geführt hat. Die Gesundheitsdirektion hat mit einem Kreisschreiben an alle Spitäler reagiert. Trotzdem ist die Rechtslage noch immer nicht umfassend geklärt.

Aus den Verträgen, die dem Datenschutzbeauftragten zur Prüfung vorgelegt wurden, geht hervor, dass Funktion, Kompetenzen, Rechte und Pflichten sowohl der Case-Manager als auch der anderen Akteure wie beispielsweise des Vertrauensarztes nicht klar definiert und in den Vereinbarungen nicht transparent aufgeführt sind. Auch weitere Unstimmigkeiten und Unklarheiten wurden von den Krankenversicherungen noch nicht behoben. Dazu gehört besonders der Informationsfluss zwischen den verschiedenen Beteiligten, der nach wie vor nicht immer nachvollziehbar ist und teilweise den massgebenden gesetzlichen Bestimmungen des Bundesgesetzes über die Krankenversicherung widerspricht.

Der Datenschutzbeauftragte regte deshalb beim Verband Zürcher Krankenhäuser an, mit den beteiligten Parteien gemeinsam einen Mustervertrag auszuarbeiten. Dieser soll eine einheitliche Handhabung des Case-Managements ermöglichen, dadurch Rechtssicherheit schaffen und eine Hilfestellung für den Abschluss solcher Verträge mit den Spitälern bieten. Der Verband Zürcher Krankenhäuser hat diese Anregung positiv aufgenommen und erste Schritte mit allen Beteiligten eingeleitet.

Datenbekanntgabe ins Ausland

Öffentliche Organe dürfen einem Empfänger im Ausland Personendaten bekannt geben, wenn die Voraussetzungen für eine Datenbekanntgabe gegeben sind und ein angemessener Schutz der übermittelten Daten gewährleistet ist. Mit dem Datenempfänger getroffene vertragliche Sicherheitsvorkehrungen zum Schutz der zu übermittelnden Personendaten sind vom öffentlichen Organ dem Datenschutzbeauftragten vorzulegen.

§ 23 IDG
§ 19 IDG
§ 22 Abs. 2 IDV

Eine Hochschule beabsichtigte, sich durch eine in den USA domizilierte Organisation akkreditieren zu lassen. Dazu hatte die Hochschule nachzuweisen, dass ihre Dozierenden den gesetzten Kriterien bezüglich ihrer Karriere und Unterhalt ihres Wissens (Forschung, Publikation, Weiterbildung etc.) entsprechen. Die Akkreditierungsstelle verlangte von der Hochschule die Bekanntgabe von Personendaten der Dozierenden wie Name und Publikationen. Die Hochschule ersuchte den Datenschutzbeauftragten um Beratung.

Für die Bekanntgabe von Personendaten ins Ausland zwecks Akkreditierung der Hochschule müssen zunächst die Voraussetzungen für eine Datenbekanntgabe erfüllt sein. Mangels gesetzlicher Grundlage war im vorliegenden Fall die Einwilligung sämtlicher betroffenen Dozierenden erforderlich. Die Einwilligung muss freiwillig, also ohne Androhung nachteiliger Konsequenzen für den Fall der Weigerung, und nach vollständiger Information erfolgen. Allfällige rechtliche Bestimmungen (gesetzliche Schweigepflichten) oder überwiegende öffentliche oder private Interessen, die der Bekanntgabe entgegenstehen, hat die Hochschule im Rahmen einer Interessenabwägung zu berücksichtigen.

Die grenzüberschreitende Übermittlung von Personendaten ist sodann nur zulässig, wenn ein angemessener Schutz der übermittelten Daten gewährleistet ist. Ein öffentliches Organ kann Personendaten einem Land, das nicht dem Europaratsübereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten untersteht, nur bekannt geben, wenn im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist, eine gesetzliche Grundlage dies erlaubt, wenn bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen sind oder vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen werden.

Ein in den USA domizilierter Empfänger gewährleistet in der Regel nur dann einen angemessenen Schutz für die Datenübermittlung, wenn er dem «Safe Harbor Agreement» beigetreten ist (siehe Staatenliste auf www.edoeb.admin.ch). Die von der Hochschule ausgewählte Akkreditierungsstelle untersteht diesem Abkommen nicht. Da auch keine gesetzliche Grundlage die Datenübermittlung erlaubte, hatte die Hochschule angemessene vertragliche Sicherheitsvorkehrungen zu treffen. Die Hochschule entwarf gestützt auf das «Swiss Transborder Data Flow Agreement» (siehe www.edoeb.admin.ch) eine separate Datenschutzvereinbarung. Der Datenschutzbeauftragte, der über die vereinbarten Sicherheitsvorkehrungen mit dem Datenempfänger zu informieren ist, hat diese Datenschutzvereinbarung für genügend befunden.

Private im Geltungsbereich des IDG

Die Bewirtschaftung kantonaler Liegenschaften ist eine öffentliche Aufgabe, welche der Regierungsrat ausschliesslich einer privatrechtlichen Aktiengesellschaft übertragen hat. Diese wurde dadurch zum öffentlichen Organ gemäss IDG und von dessen Geltungsbereich erfasst.

§ 3 Abs. 1 lit. c. IDG
Art. 38 i.V.m. Art. 98 KV
§ 6 IDG i.V.m. § 25 IDV
§ 2 Abs. 2 IDG

Verwaltung und Gemeinden lagern immer mehr Aufgaben an verwaltungsexterne Organisationen und Personen aus. So lässt der Kanton beispielsweise seine Liegenschaften durch die privatrechtlich organisierte Kantag Liegenschaften AG bewirtschaften. Die Liegenschaften, die sie verwaltet, gehören weitgehend zum kantonalen Finanz- und Verwaltungsvermögen oder stehen im Eigentum der Personalvorsorgestiftung des Kantons.

Organisationen und Personen des öffentlichen und privaten Rechts gelten als öffentliche Organe im Sinne des IDG, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind. Die Bewirtschaftung kantonaler Liegenschaften stellt eine öffentliche Aufgabe dar. Diese wurde der Kantag mit Beschluss des Regierungsrates vom 2. September 1988 übertragen. Die Kantag stellt somit selber ein öffentliches Organ im Sinne des IDG dar und ist deshalb für den Umgang mit Informationen eigenverantwortlich. Gemäss Kantonsverfassung werden kantonale oder kommunale Aufgaben einer Organisation oder Person per Gesetz übertragen. Wird einer Organisation die Erfüllung einer öffentlichen Aufgabe hingegen lediglich im Rahmen eines Auftrags übertragen («Outsourcing»), wird diese deswegen nicht automatisch zu einem öffentlichen Organ. Die Verantwortung für den Umgang mit Informationen bleibt grundsätzlich beim Gemeinwesen. Das IDG kommt hier insoweit zur Anwendung, als die Organisation im Rahmen der Auftragserfüllung Informationen des Gemeinwesens bearbeitet.

Auch wenn eine Organisation wie die Kantag als öffentliches Organ zu qualifizieren ist, würde sie nicht in den Anwendungsbereich des IDG fallen, sofern sie am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt. Die Bewirtschaftung kantonaler Liegenschaften wurde mit vorerwähntem Regierungsratsbeschluss ausschliesslich der Kantag zugewiesen. Ein Submissionsverfahren wurde seinerzeit soweit ersichtlich nicht durchgeführt. In Bezug auf die Bewirtschaftung dieser Liegenschaften steht die Kantag daher nicht im wirtschaftlichen Wettbewerb mit anderen, insbesondere privaten Anbietern von Liegenschaftenbewirtschaftungen. Dass die Kantag für eine vollständige und wirtschaftlich optimale Vermietung der kantonalen Liegenschaften nach marktwirtschaftlichen Grundsätzen zu sorgen hat, ändert daran nichts. Die Kantag wird somit vollständig vom Anwendungsbereich des IDG erfasst. Die Finanzdirektion, bei welcher die Kantag administrativ angegliedert ist, hat sich dieser Meinung angeschlossen.

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

Strategische Einheit
lic. iur. Beda Harb, Stv. Datenschutzbeauftragter
lic. iur. Beatrice Glaser

Operative Einheit
lic. iur. Veronica Blattmann, Stv. Datenschutzbeauftragte
lic. iur. Karin Brunner Steib
lic. iur., RA Claudio Fäh
lic. iur., RA Monika Lüscher
lic. iur. Barbara Mathis
Reto Mathys, Dipl. Ing. FH
Andrea Carlo Mazzocco, CISA

Kommunikation/Aus- und Weiterbildung
Dr. phil. Andrea Ruf

Dienstleistungen
Martina Richard
Susanne Brüngger

Tätigkeitsbericht 2009 (ab 1.10.2008)
ISSN 1422-5816

Design
Giger & Partner, Zürich

Layout
Schulthess Juristische Medien AG, 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

Datenschutz
mit Qualität

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Tel.: 043 259 39 99
Fax: 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch