Tätigkeitsbericht

2010

dsb
datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter Kanton Zürich

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. Er führt Kontrollen durch, beurteilt datenschutzrelevante Vorhaben und Erlasse, berät die verantwortlichen Organe, bietet Aus- und Weiterbildungen im Bereich Datenschutz an und fördert den Einsatz datenschutzfreundlicher Technologien. Dabei kann er verbindliche Empfehlungen abgeben.

Der Datenschutzbeauftragte informiert und sensibilisiert die Öffentlichkeit für die Anliegen des Datenschutzes und der Informationssicherheit. Er berät Privatpersonen und vermittelt in Konfliktfällen. Alle Aufgaben nimmt der Datenschutzbeauftragte in vollständiger Unabhängigkeit wahr. Er leistet damit einen wichtigen Beitrag für den Erhalt eines der zentralen Grundrechte einer liberalen Gesellschaft: das Recht auf den Schutz der Privatsphäre.

Tätigkeitsbericht 2010

Der Beauftragte 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 IDG).
Der vorliegende Tätigkeitsbericht ist der zweite, der sich nach dem Gesetz über die Information und den Datenschutz (IDG) richtet, das am 1. Oktober 2008 in Kraft getreten ist.
Der Bericht deckt den Zeitraum vom 1. Januar 2010 bis und mit 31. Dezember 2010 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2011

Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Zwischen Anspruch und Wirklichkeit

Bürgerinnen und Bürger betonen in Umfragen regelmässig, wie wichtig ihnen der Schutz ihrer Privatsphäre ist. Dabei zeigen sie grosses Vertrauen in die staatlichen Datenbearbeiter. In der informatisierten Verwaltung mit zunehmend komplexeren Arbeitsabläufen ist dieses Vertrauen nicht ohne Anstrengungen zu erhalten.

Verschiedene Gesetzesvorhaben mit unterschiedlichen Datenbearbeitungen gehörten im vergangenen Jahr zu den Schwerpunkten der Tätigkeit des Datenschutzbeauftragten. In der Hektik des Alltags geht oftmals vergessen, dass der Schutz der Privatsphäre zu den wesentlichen Errungenschaften unserer liberalen Rechts- und Wirtschaftsordnung gehört. Bereits die Europäische Menschenrechtskonvention (EMRK) hält diesen Anspruch auf Privatsphäre fest, und die Bundesverfassung garantiert das Grundrecht auf persönliche Freiheit und Datenschutz.

Für die öffentlichen Organe bedeutet dies, dass sie das Recht auf Privatheit der Bürgerinnen und Bürger nur dann einschränken dürfen, wenn es einerseits im öffentlichen Interesse liegt und andererseits für die Aufgabenerfüllung des Staates geeignet und erforderlich ist. Das Legalitätsprinzip verlangt folglich, dass die Regelung auf einer entsprechenden Rechtsgrundlage erfolgt.

Eingriff in die persönliche Freiheit

Jedes Bearbeiten von Personendaten bedeutet einen Eingriff in die persönliche Freiheit und die Privatsphäre. Es ist deshalb die Aufgabe des Gesetzgebers, Rechtsgrundlagen zu schaffen, die den verfassungsmässigen Anspruch auf Privatheit respektieren. Die Anforderungen an den Gesetzgeber sind in Bezug auf die Regelung von Datenbearbeitungen in den letzten Jahren enorm gestiegen. Einerseits bringt die Informatisierung der Verwaltung immer neue Möglichkeiten der Datenbearbeitungen und des Datenaustauschs, während andererseits die Anforderungen an die Behörden aufgrund zunehmend komplexerer Aufgaben gestiegen sind. In dieser Situation den Überblick zu behalten und die grundrechtlichen Anliegen der Bürgerinnen und Bürger zu respektieren, ist eine grosse Herausforderung. Im vergangenen Jahr hat der Datenschutzbeauftragte verschiedentlich zu Gesetzgebungsvorhaben Stellung bezogen, die exakt von dieser Ausgangslage geprägt sind. Dabei sind die Datenschutzbestimmungen nicht die zentralen Fragen der jeweiligen Gesetzgebung, aber für die Wahrung der Privatsphäre der Bürgerinnen und Bürger sind sie entscheidend.
Das Pflegefinanzierungsgesetz als eines dieser Gesetze zeigt exemplarisch, wie der Anspruch und die Wirklichkeit in Bezug auf den Schutz der Privatsphäre der betroffenen Personen auseinanderklaffen können.

Sensible Gesundheitsdaten

Auf den Punkt gebracht: Jede Person, die Pflegeleistungen bezieht, muss jederzeit damit rechnen, dass ihre patientenbezogenen Daten von der Gesundheitsdirektion oder einer Gemeinde eingesehen werden können. So kam es im vergangenen Jahr auch schon vor, dass eine Gemeindemitarbeiterin von der Diagnose ihres Vorgesetzten erfuhr.

Selbstverständlich sind die im Pflegegesetz vorgesehenen Datenbearbeitungen auf die zum Vollzug der Gesetzgebung notwendigen Daten beschränkt. Ist es aber notwendig, dass alle diese Informationen von den Pflegeheimen und Spitexdiensten in nicht anonymisierter Form an die Gesundheitsdirektion oder Gemeinden fliessen, oder sogar von Dritten erhoben werden können, und erst bei einer allfälligen Publikation von der Direktion anonymisiert werden müssen?

Angaben zur Gesundheit einer Person sind besondere Personendaten nach dem Informations- und Datenschutzgesetz (IDG). Sie sind Teil der intimen Daten eines Menschen und deshalb besonders zu schützen, da das Risiko einer Persönlichkeitsverletzung sehr hoch ist. Werden solche Daten bearbeitet, ist ebenso zu beachten, dass dies transparent für die betroffenen Personen geschieht, damit diese jederzeit auch ihre Persönlichkeitsrechte wahrnehmen können.

Das IDG formuliert hierzu die Rahmenbedingungen. Die gesetzliche Grundlage muss bei besonderen Personendaten hinreichend bestimmt sein. Dies bedeutet, dass es klar sein muss, wer für die Datenbearbeitung verantwortlich ist, zu welchen Zwecken die einzelnen Datenbearbeitungen erfolgen und welche Datenkategorien betroffen sind. Mit der Festlegung dieser Eckpunkte lässt sich beurteilen, welche Datenbearbeitungen damit geeignet und erforderlich sind. Eine generalklauselartige Formulierung vermag diesen Anforderungen nicht zu genügen, wie dies das Bundesgericht auch in Bezug auf die Bestimmungen zur Videoüberwachung im Polizeigesetz feststellte – und Letztere folglich aufhob.

Generalklauseln mit Risiken

Mit Generalklauseln lassen sich hier die rechtsstaatlichen Anforderungen an den Schutz der Privatsphäre nicht erfüllen. Sie verunsichern aber auch die verantwortlichen Organe, da diese nicht klar aus dem Gesetz erkennen können, welche Eingriffe in die Persönlichkeitsrechte der betroffenen Personen zulässig sind. Jede rechtswidrige Datenbearbeitung kann aber auch für den einzelnen Mitarbeitenden strafrechtliche Konsequenzen haben, da sie eine Verletzung des Amts- oder Berufsgeheimnisses beinhalten kann. Der Anspruch der Bürgerinnen und Bürger auf Schutz ihrer Privatsphäre erfordert transparente Rechtsgrundlagen. Wenn nicht mehr klar ist, welche Organe welche Daten über die einzelnen Personen bearbeiten, schwindet auch das bestehende Vertrauen in die Datenbearbeitungen der öffentlichen Organe. Aber auch die Verwaltungsstellen sind auf klare gesetzliche Bestimmungen angewiesen, um mit den notwendigen und definierten Datenbearbeitungen ihre Aufgaben effizient erfüllen zu können.

Nachhaltiger Schutz der Privatsphäre

Die gesetzliche Aufgabe des Datenschutzbeauftragten ist es, durch Beratungen und Kontrollen den Anliegen des Schutzes der Privatsphäre der Bürgerinnen und Bürger Nachachtung zu verschaffen. Im letzten Jahr hat sich gezeigt, dass es bei der Gesetzgebung immer wichtiger wird, klare Regelungen zu finden, die die Datenbearbeitungen transparent machen. Es darf nicht dazu kommen, dass Anspruch und Wirklichkeit immer mehr auseinanderklaffen – im Interesse der Bürgerinnen und Bürger sowie der verantwortlichen Organe.

Weitere Schwerpunkte in den verschiedenen Tätigkeitsbereichen

- Kontrolltätigkeit: Staatsschutz
- Beratung öffentlicher Organe: Reglemente zur Videoüberwachung
- Beratung Privatpersonen: Individualrechte
- Beurteilung technischer Vorhaben: Outsourcing
- Vorabkontrollen: Data Mining

Datenschutzthemen von morgen

Der Tätigkeitsbericht gibt jeweils eine Momentaufnahme der aktuellen Datenschutzthemen. Die zukünftigen Herausforderungen zeichnen sich aber bereits heute ab.

In verschiedenen Bereichen werden besonders sensitive Personendaten bearbeitet, so zum Beispiel im Gesundheitswesen. Mit dem medizinischen Fortschritt werden bei der Behandlung zunehmend genetische Informationen verwendet. Solche Daten gehören zu den intimsten Informationen eines Menschen und bergen ein hohes Diskriminierungspotenzial in der Gesellschaft. Darüber hinaus können sie nicht nur Informationen über eine Person, sondern auch über weitere verwandte Personen umfassen. Die Spitäler werden besonders angehalten sein, den Schutz dieser – unter dem Arzt- und Patientengeheimnis stehenden – Informationen zu gewährleisten. Hierfür müssen sie über klinische Informationssysteme verfügen, die den Datenschutz und die Sicherheit vollumfänglich gewährleisten. Regelmässige Kontrolle durch den Datenschutzbeauftragten – entsprechende Ressourcen vorausgesetzt – müssen die Verlässlichkeit dieser sensitiven Systeme überprüfen können. Des Weiteren wird im Gesundheitswesen darauf zu achten sein, dass sensitive Gesundheitsdaten nicht an Dritte weitergegeben werden, ohne dass eine unbedingte Notwendigkeit besteht. Verschiedene Tendenzen zeigen, dass das Arzt- und Patientengeheimnis immer mehr aufgeweicht wird und im Rahmen von Gesetzgebungen, die andere Ziele verfolgen, auch Gesundheitsdaten übermittelt werden, so beispielsweise im Bereich der Pflege- und der Spitalfinanzierung. Aber auch die Krankenversicherer wollen immer mehr Gesundheitsdaten und verlangen in Tarifverträgen auch medizinische Informationen. Um das Arzt- und Patientengeheimnis auch in Zukunft zu wahren, wird vermehrt darüber zu diskutieren sein, ob Finanzierungen oder Wirtschaftlichkeitsüberprüfungen nicht auch auf der Basis von anonymisierten Daten erfolgen können.

Sensitive Überwachungsmassnahmen

Die Videoüberwachung stellt eine von verschiedenen Überwachungsmöglichkeiten von Personen dar. Eine Regelung der Videoüberwachung hat für die Bürgerinnen und Bürger klar zu sein. Das Bundesgericht hat einen Paragrafen zur Videoüberwachung im Polizeigesetz aufgehoben. Es war nicht klar, wo, wann und zu welchen Zwecken eine solche Überwachung stattfinden soll. Aber auch die weiteren Rahmenbedingungen waren zu wenig eindeutig geregelt. Videoüberwachung und andere Überwachungsmassnahmen dürften auch in Zukunft noch zunehmen. Die Überwachung wird es erlauben, auch Gespräche aufzunehmen oder bei bestimmtem Verhalten weitere Informationen abzufragen oder einen Alarm auszulösen. Es wird deshalb in Zukunft darüber zu entscheiden sein, welche Art der Überwachung notwendig ist und wie sie eingegrenzt werden soll, damit nicht eine dauernde und flächendeckende Überwachung der gesamten Bevölkerung erfolgt.

Umfassende Betreuung

Im Sozialbereich hat das Bedürfnis zugenommen, Personen umfassend und durch mehrere Stellen gleichzeitig betreuen zu können. Vielfach sind die zu betreuenden Personen in verschiedenen Bereichen mit den staatlichen Stellen in Kontakt, beispielsweise im Schulbereich, bei der Jugend- und Familienhilfe, beim Sozialamt oder bei der IV-Stelle. Dabei haben alle Stellen das Interesse, die Probleme so rasch wie möglich und unter Berücksichtigung möglichst aller Aspekte zu lösen. In allen diesen Bereichen fallen zum Teil sehr sensitive persönliche Informationen an. Werden diese Daten zusammengenommen, entstehen eigentliche Persönlichkeitsprofile.

Um die (Re-)Integration dieser Personen in die Gesellschaft zu ermöglichen, ist es entscheidend, dass Informationen nicht an unbefugte Dritte gelangen. Es wird deshalb zunehmend wichtig, dass klar definiert wird, wer über welche Informationen verfügen soll. Zudem stellt sich die Frage, wie betroffene Stellen in diesem Bereich erweiterten Geheimhaltungsvorschriften unterstellt werden können, wie dies beispielsweise bei der Opferhilfe schon heute der Fall ist.

Elektronische Interaktion

In Zukunft wird der Bürger immer mehr die Möglichkeit haben, mit dem Staat elektronisch zu kommunizieren. Bereits heute können Dienstverschiebungsgesuche elektronisch eingereicht werden und in naher Zukunft wird dies auch für die Steuererklärung der Fall sein. Solche interaktiven Plattformen müssen die Sicherheit bieten, dass die persönlichen Daten der Bürgerinnen und Bürger nicht in unbefugte Hände geraten. Die Verfügbarkeit, die Vertraulichkeit und die Integrität, aber auch die Nachvollziehbarkeit von solchen Datentransfers müssen garantiert sein. Werden im Rahmen des E-Governments weitere Massnahmen geplant, wird insbesondere diesen Punkten Nachachtung zu verschaffen sein.

Aber auch bei der Verwendung anderer neuer Technologien wird sich der Staat fragen müssen, wie weit die Privatheit der Bürgerinnen und Bürger garantiert ist. Sollen Bemühungen um das «Open Government» weiter vorangetrieben werden – erste zaghafte Schritte sind die Verwendung von Sozialen Netzwerken für die Informationsverbreitung –, ist auch sicherzustellen, dass die Anliegen auf Schutz der Privatheit mitberücksichtigt werden.

Komplexere Gesetzgebungen

Viele Gesetzgebungen beinhalten auch Informationsflüsse. Dabei stehen die Anliegen des Schutzes der Privatheit der Bürgerinnen und Bürger nicht im Zentrum, sondern sind Teil einer Gesetzgebung, die einen anderen Kern hat. Dennoch ist gerade für den Schutz der Privatsphäre dieser Teil entscheidend, denn er wird sich wie das Teil eines Puzzles in den gesamten Schutz der Privatheit der Bürgerinnen und Bürger einfügen. Deshalb stellt sich immer wieder die gleiche Frage: Wer benötigt welche Daten zu welchem Zweck? Angesichts der zunehmend komplexeren Sachverhalte der Gesetzgebung ist dies aber keine einfache Frage. Insbesondere unter dem Aspekt des Schutzes der persönlichen Freiheit der Bürgerinnen und Bürger muss in jedem Einzelfall die Frage gestellt werden, ob ein Datenfluss auch geeignet und erforderlich ist. Vielfach lässt sich der Zweck der Datenbearbeitung klarer formulieren und damit auch genauer bestimmen, welche Datenkategorien erforderlich sind. Oder es stellt sich heraus, dass das Ziel auch mit anonymisierten Daten zu erreichen ist. Die Wahrung der Grundrechte als Ziel der Verfassung und als konkretisierte Materie im IDG gehört auch in Zukunft zu den Hauptanliegen des Gesetzgebers. Die Bürgerinnen und Bürger haben hierauf Anspruch, und sie wollen Transparenz, was mit ihren Daten geschieht. Auch wenn er unter dem Amtsgeheimnis steht, sollten auf dem Tisch des Gemeindeschreibers in Zukunft nicht noch mehr Gesundheitsdaten über seinen Chef landen.

Wirkung des Gesetzes

Das IDG bewegt sich in einem dynamischen Umfeld zwischen technologischen Entwicklungen, die den Datenschutz, und gesellschaftlichen Entwicklungen, die den Umgang mit Informationen betreffen.

Der Gesetzgeber hat dem Datenschutzbeauftragten die Aufgabe übertragen, im Rahmen seiner Berichterstattung auch über die Wirkung des Gesetzes zu berichten. Im Tätigkeitsbericht 2009 erfolgte erstmals eine diesbezügliche Auslegeordnung. Die damalige Feststellung, dass es rund ein Jahr nach Einführung des Gesetzes noch zu früh sei, die Wirkung zu analysieren, trifft auch nach rund zwei Jahren IDG zu.

Revision des IDG

Sowohl im Bereich des Datenschutzes wie auch beim Informationszugang zeigt sich, dass verschiedene Gesetzesbestimmungen in der praktischen Umsetzung zu Fragen Anlass geben. Es kann indessen noch nicht beurteilt werden, ob es sich hier um Einzelfragen handelt oder ob sich eine Präzisierung der Gesetzgebung aufdrängt. Der Datenschutzbeauftragte erfasst diese Problemstellungen systematisch, um die Bereiche festlegen zu können, in denen sich ein gesetzgeberischer Handlungsbedarf aufdrängt. Es ist dabei nicht ungewöhnlich, dass im Umfeld der technologischen und gesellschaftlichen Entwicklungen Revisionen des IDG ins Auge gefasst werden müssen. Einerseits zeigen sich auf europäischer Ebene Entwicklungen, die aufgrund der Verträge der Schweiz mit der EU auch auf die kantonale Gesetzgebung Auswirkungen haben werden, andererseits ersieht man auch aus den neueren Gesetzgebungen im Bund und in anderen Kantonen, dass Anpassungen notwendig sein werden. Es ist indessen ratsam, diese Entwicklungen in eine Gesamtbetrachtung des IDG einzuordnen.

Schwierige Datenbekanntgabe

Seit Inkrafttreten des IDG ist es bereits zu Änderungen des Gesetzes gekommen, die aus anderen Kontexten her veranlasst wurden. Sie betreffen die Bekanntgabe von Personendaten (§ 16 und 17 IDG), die Stellung des Datenschutzbeauftragten (§ 30 IDG) sowie den Rechtsschutz (§ 39a IDG).

Insbesondere die neue Bestimmung zur Bekanntgabe von Personendaten (§ 16 Abs. 1 lit. c und § 17 Abs. 1 lit. c) stellt im System der Bekanntgabe von Personendaten eine schwierige Ausgangslage für die Praxis dar und ist für die verantwortlichen Verwaltungsstellen kaum umzusetzen. Die eingefügte Formulierung, dass im Einzelfall die Bekanntgabe von – auch besonderen – Personendaten möglich sein soll, wenn «der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist», soll eine Weiterleitung von Personendaten immer dann ermöglichen, wenn eine Interessenabwägung dafür spreche. Einerseits liegt damit eine generalklauselartige Formulierung vor, die insbesondere bei der Bekanntgabe von besonderen Personendaten fragwürdig ist; andererseits wird als Voraussetzung für die Datenbekanntgabe eine Interessenabwägung verlangt. Die klaren Regelungen und die Systematik des IDG für die Bekanntgabe von Personendaten werden damit durchbrochen: Es ist nicht definiert, in welchen Fällen welche wesentlichen Rechtsgüter gegenüber den Grundrechten der betroffenen Personen (§ 1 IDG) höher zu gewichten sind. Im Zweifelsfall wird sich ein verantwortliches Organ gegen eine Datenbekanntgabe entscheiden müssen, um nicht das Amtsgeheimnis zu verletzen.

Es ist deshalb wünschbar, von isolierten Revisionen des IDG abzusehen und Anpassungen im Rahmen einer Gesamtbetrachtung vorzunehmen, welche die Wirkung des Gesetzes mit beinhaltet.

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 08	B 09	Δ(P 10)	P 10	Δ(P 11)	P 11	Δ(P 12)	P 12	P 13	Δ%(08-13)
Ertrag	0.0	0.2	0.0	0.2	0.0	0.0	0.0	0.0	0.0	
Aufwand	-1.7	-2.1	0.0	-2.2	0.0	-2.2	-0.0	-2.2	-2.3	35.9
Saldo	-1.7	-1.9	0.0	-2.0	0.0	-2.2	-0.0	-2.2	-2.2	
Investitionen (in Mio. Fr.)										Ø (08 -13)
Einnahmen										
Ausgaben	-0.0	0.0	-0.1	-0.1	0.0		0.0			-0.0
Nettoinvestitionen	-0.0	0.0	-0.1	-0.1	0.0		0.0			-0.0
Personal (Beschäftigungsumfang)	7.3	8.2	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	Aufsicht: Aufbau eines Monitorings (konzeptionelle Weiterentwicklung und Standardisierung der Prozesse)	2011	0
E2	Kontrolle: Verstärkung in den Bereichen "Bearbeitung besonderer Personendaten" und "Schengen"	2010	0
E3	Datenschutzfreundliche Technologien: Förderung der Entwicklung und des Einsatzes von datenschutzfreundlichen Technologien	2011	0

Indikatoren

		Art	R 08	B 09	P 10	P 11	P 12	P 13
Wirkungen								
W1	Anteil umgesetzter Empfehlungen	P		60 %	60 %			
W2	Kundenbeurteilung der Qualität der Leistungen	min.		gut	gut			
W3	Anteil umgesetzter Hinweise	P		60 %	60 %			
Leistungen								
L1	Anteil komplexer Beratungen von öffentlichen Organen	P		33 %	33 %			
L2	Anteil aufwändiger Beratungen von Privatpersonen	P		15 %	15 %			
L3	Anzahl Grundsatzfragen u. Stellungnahmen	max.		25	25			
L4	Anzahl Datenschutz-Reviews	min.		20	20			
L5	Zuwachs Besuche auf Internetangeboten	P		5 %	5 %			
L6	Anzahl Teilnehmerstunden an Weiterbildungsangeboten	min.		600	600			
Wirtschaftlichkeit								

Leistungsgruppe 9071	Budgetentwurf 2010
Budgetkredit Erfolgsrechnung (in Mio Fr.)	-1.991
Budgetkredit Investitionsrechnung (in Mio. Fr.)	-0.070
Leistungsindikatoren L3, L4 und L6	

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

Anhang 1-10

Im stetigen Austausch mit der Verwaltung

Im Berichtsjahr wurden mehrere hundert datenschutzrechtliche Anfragen von öffentlichen Organen bearbeitet. Während sich die Anfragen kantonaler Institutionen meist auf komplexe datenschutzrechtliche Fragestellungen zu ganz unterschiedlichen Themenbereichen bezogen, bildete bei den Gemeinden die datenschutzkonforme Regelung von Videoüberwachungen einen Schwerpunkt.

Eine der zentralen Aufgaben des Datenschutzbeauftragten ist die Unterstützung und Beratung der öffentlichen Organe in Fragen des Datenschutzes. Darunter fallen neben den Direktionen und ihren Ämtern auch die selbständigen öffentlich-rechtlichen Anstalten wie die Elektrizitätswerke des Kantons Zürich (EKZ), die Gebäudeversicherung (GVZ) oder die Sozialversicherungsanstalt (SVA), die öffentlichen Spitäler wie das Kantonsspital Winterthur oder das Universitätsspital sowie die Bildungsinstitutionen, die Universität und die Fachhochschulen. Die Bezirke sowie alle Gemeinden, die über keinen unabhängigen Datenschutzbeauftragten verfügen – das sind ausser Zürich und Winterthur alle 169 Kommunen – fallen ebenfalls in den direkten Zuständigkeitsbereich des Datenschutzbeauftragten.

Aufwändige Beratungsmandate und gezielte Kurzberatungen

Die Anfragen öffentlicher Organe lassen sich grundsätzlich in zwei Kategorien einteilen: Einerseits die Bearbeitung aufwändiger Beratungsmandate zu komplexen datenschutzrechtlichen Fragestellungen, die in der Regel eine aktive, oft mehrmonatige Mitarbeit des Datenschutzbeauftragten in einer Arbeitsgruppe im Rahmen eines Gesetzgebungsvorhabens, eines Vernehmlassungsverfahrens oder eines Informatikprojekts erfordert; andererseits die Kurzberatungen per E-Mail oder Telefon, die eine Analyse der jeweiligen Rechtslage sowie das Aufzeigen der Möglichkeiten beinhalten, eine beabsichtigte Datenbearbeitung datenschutzkonform vorzunehmen. Dabei lässt sich feststellen, dass die Beratungsmandate für kantonale Institutionen rund drei Viertel der zeitlichen Ressourcen im Bereich Beratung in Anspruch nehmen, während die Kurzberatungen mit rund einem Viertel zu Buche schlagen.

Breite Themenpalette bei Beratung öffentlicher Organe

Bei den Beratungen kantonaler Institutionen lagen die thematischen Schwerpunkte im Berichtsjahr in den Bereichen Gesundheitswesen und E-Government. Ausserdem wurden mehrere Beratungsmandate aus dem Schul- und Sozialwesen bearbeitet.

Datenschutzkonforme Videoüberwachung beschäftigt viele Gemeinden

Einen thematischen Schwerpunkt der Anfragen aus Gemeinden bildete, wie bereits im Vorjahr, die datenschutzkonforme Regelung von Videoüberwachungen. Ob in der Schule, durch die Polizei oder im öffentlichen Verkehr, Videoüberwachung kommt in unserem Alltag immer öfter zum Einsatz. Die Breite der Fragestellungen bezüglich Videoüberwachung, mit denen der Datenschutzbeauftragte 2010 durch die Gemeinden konfrontiert wurde, lässt sich auf den Seiten 18 und 19 dieses Tätigkeitsberichts nachvollziehen.

Neues Personalinformationssystem PULS-ZH

Seit dem 1. Januar 2011 ersetzt das neue Personalmanagement- und Lohnadministrationssystem PULS-ZH das bisherige Personalinformationssystem PALAS. Die datenschutzrechtlichen Anforderungen an das System sind jedoch noch nicht umgesetzt.

Im Januar 2009 beschloss der Regierungsrat, das Personalinformationssystem PALAS durch ein neues System zu ersetzen. Unter der Bezeichnung «Personalmanagement- und Lohnadministrationssystem PULS-ZH» wurden die Projektarbeiten für ein solches System an die Hand genommen. Bei PULS-ZH handelt es sich um das weit verbreitete Standardsystem SAP HCM. Die Ablösung des alten Systems erfolgte auf den 1. Januar 2011.

Mehrmalige Stellungnahmen des Datenschutzbeauftragten

Der Datenschutzbeauftragte nahm zum Projekt PULS-ZH mehrmals Stellung. Er wies erstmals im März 2009 darauf hin, dass im Hinblick auf den Datenschutz noch ein grosser Handlungsbedarf bestehe. Daran änderte sich im Verlauf der Entwicklung des Projekts wenig, so dass wichtige Dokumente zum Zeitpunkt der produktiven Inbetriebnahme des Systems immer noch nicht vorhanden waren und verschiedene datenschutzrechtlich relevante Themen zwar andiskutiert, aber weder rechtlich noch technisch gelöst waren.

Entsprechend verlangte der Datenschutzbeauftragte von der Projektleitung einen verbindlichen Zeitplan für die Ausarbeitung von genügenden Rechtsgrundlagen. Zudem sollte die Projektleitung den Datenkatalog transparent vorlegen und die Prozesse, die in PULS-ZH durchgeführt werden können, abschliessend darstellen. Auch über die Einhaltung der Sicherheitsanforderungen für das System forderte der Datenschutzbeauftragte Klarheit. Und schliesslich wies er die Projektleitung auf verschiedene Problemkreise hin, für die noch eine Lösung gefunden werden musste, wie beispielsweise die Übergabe und Archivierung der digitalen Akten an das Staatsarchiv oder auch die technische Löschung der Daten im System PULS-ZH.

Datenschutzkonforme Implementierung zugesagt

Die Projektleitung von PULS-ZH sicherte gegenüber dem Datenschutzbeauftragten Ende 2010 verbindlich zu, dass die Umsetzung der datenschutzrechtlichen Anforderungen im Verlauf des Jahres 2011 erfolgen wird. Damit kann – im Nachhinein – ein datenschutzkonformer Betrieb sichergestellt werden. Der Datenschutzbeauftragte wird die Einhaltung dieser Zusicherungen überprüfen und sich allenfalls erneut dazu äussern. Auch behält er sich vor, eine Kontrolle des Systems PULS-ZH durchzuführen.

Personalgesetz

§ 8 Abs. 2 IDG

Information der Schulbehörden über Delikte Jugendlicher

Mit einer Weisung hat die Jugendstaatsanwaltschaft die Informationsflüsse an die Schulbehörden bei bestimmten Delikten konkretisiert. Diese Regelung stützte sich bis Ende 2010 auf eine Bestimmung in der Strafprozessordnung.

Die Weisung der Jungendstaatsanwaltschaft konkretisiert die Informationsmöglichkeiten der Jugendanwälte im Strafverfahren gegen Jugendliche, die eine Schule besuchen. Sie hält fest, wann eine Mitteilung an die Schulbehörden verhältnismässig ist. Die Regelung stützt sich auf eine Bestimmung der kantonalen Strafprozessordnung, die Ende 2010 mit Einführung der eidgenössischen Strafprozessordnung aufgehoben wurde.

Kein systematischer Datenaustausch

In Beantwortung einer kantonsrätlichen Anfrage sprach sich der Regierungsrat für die Weiterführung dieser Weisung aus. Sie könne neu auf das IDG abgestützt werden, das Datenbekanntgaben nach einer Interessenabwägung im Einzelfall ermögliche. Ein systematischer Informationsaustausch sei hingegen nicht zulässig. Die Erfahrungen der nächsten Jahre würden zeigen, ob ein Bedürfnis nach einer Gesetzesgrundlage für umfassendere Mitteilungen bestehe.

Gesetzliche Grundlage notwendig

Grundsätzlich ist mit dem Regierungsrat festzuhalten, dass eine systematische Information der Schulbehörden nur aufgrund einer gesetzlichen Grundlage möglich ist. Der als Rechtsgrundlage herangezogene Paragraf des IDG regelt ausschliesslich den Einzelfall und ermöglicht eine aktive Information dann, wenn der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist. Für voraussehbare regelmässige Mitteilungen hingegen sind klare gesetzliche Bestimmungen zu erlassen. Die Information der Schulbehörden führt zu einer regelmässigen Datenbekanntgabe in einer Vielzahl von Fällen und ist daher separat zu regeln.

So wichtig die Mitteilungen zum Schutz anderer Rechtsgüter sein können, so sorgfältig ist darauf zu achten, dass die Persönlichkeitsrechte der verdächtigten Jugendlichen – in diesem Verfahrensstadium ist auch die Unschuldsvermutung zu berücksichtigen – gewahrt werden. Wenn es sich, wie im vorliegenden Fall, um die Weitergabe von besonderen Personendaten handelt, ist eine separate Regelung auf Gesetzesstufe unerlässlich.

§ 16 Abs. 1 lit. c IDG

§ 17 Abs. 1 lit. c IDG

§ 379 Strafprozessordnung Kanton Zürich

Sozialhilfegesuch mit Foto?

Zur besseren Wiedererkennung von Sozialhilfebezügerinnen und Sozialhilfebezügern im Alltag möchte eine Gemeinde die Gesuchstellenden verpflichten, mit dem Sozialhilfeantrag ein Foto oder eine Ausweiskopie einzureichen. Eine rechtliche Grundlage dazu fehlt jedoch im Sozialhilfegesetz.

Eine Gemeinde liess im Berichtsjahr beim Datenschutzbeauftragten abklären, ob es möglich wäre, Sozialhilfegesuchsteller zu verpflichten, zusammen mit dem Gesuch um wirtschaftliche Sozialhilfe ein Foto einzureichen. Dies sollte eine bessere Wiedererkennung der Personen auf der Strasse oder beim Einkauf ermöglichen und dadurch zur Missbrauchsbekämpfung beitragen.

Foto zur Prüfung des Sozialhilfebedarfs nicht notwendig

Eine Sozialhilfebehörde darf nur diejenigen Daten erheben, die für die Abklärung des Anspruchs auf finanzielle Unterstützung gemäss dem Sozialhilfegesetz notwendig sind. Die Fotografie einer Person ist bei der Beurteilung, ob ein solcher Unterstüt-zungsbedarf vorliegt, weder geeignet noch erforderlich.

Es gehört nicht zu den Aufgaben der Mitarbeiterinnen und Mitarbeiter einer Sozialhilfebehörde, ausserhalb ihrer Arbeitszeit Sozialhilfebeziehende zu beobachten und mögliche Missbräuche zu ermitteln. Bei einem Verdacht auf Missbrauch klärt das Sozialamt den Sachverhalt von Amtes wegen ab und kann mittels Amtshilfe Informationen über die Gesuchstellerin oder den Gesuchsteller bei anderen Behörden einholen. Bei Bedarf ist es ausserdem möglich, Mitarbeitende oder eine Drittperson als Sozialhilfeinspektorin beziehungsweise Sozialhilfeinspektor zu beauftragen und einzusetzen.

§ 8 Abs. 1 IDG

§ 7 Sozialhilfegesetz

§ 33 Verordnung zum Sozialhilfegesetz

Vorabkontrollen: Data Mining in der Verwaltung

Im Rahmen einer Vorabkontrolle überprüft der Datenschutzbeauftragte die Tragweite des Eingriffs in die Persönlichkeitsrechte und die gesetzlichen Grundlagen. Von Bedeutung sind Datenkategorie und Art der Datenbearbeitung sowie die geplanten Schutzmassnahmen. 2010 wurden in einer formellen Vorabkontrolle die Voraussetzungen für ein Data-Mining-Projekt in der Verwaltung geprüft.

Bei den meisten im Berichtsjahr zur Vorabkontrolle eingereichten Vorhaben wünschten öffentliche Organe Zugriff auf Personendaten eines anderen öffentlichen Organs, und zwar mit der Begründung, die Daten zur Erfüllung ihrer gesetzlichen Aufgaben zu benötigen. Die beiden nachfolgend präsentierten Projekte illustrieren diese Ausgangslage exemplarisch.

Zugriff des Betreibungsamtes aufs Einwohnerregister

Betreibungsämter verlangten, eine elektronische Abrufmöglichkeit von Daten aus den Einwohnerregistern der dem Betreibungskreis zugehörigen Gemeinden zu erhalten. Die besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen liegen bei einem Onlinezugriff darin, dass die Empfängerstelle befugt wird, ohne Einflussmöglichkeit des bekanntgebenden Organs auf Daten einer Vielzahl von Bürgerinnen und Bürgern zuzugreifen. Obschon das geplante Vorhaben das Recht auf informationelle Selbstbestimmung der Betroffenen beschränkt, erachtete der Datenschutzbeauftragte den Eingriff in die Persönlichkeitsrechte aufgrund der Art der Daten und des eingeschränkten Zugriffs als gering. Er verzichtete deshalb auf die Durchführung einer formellen Vorabkontrolle. Im Rahmen seiner Beratungsfunktion machte er die anfragende Behörde darauf aufmerksam, dass das zürcherische Gemeindegesetz die Möglichkeit vorsieht, einem öffentlichen Organ Zugriff auf das Einwohnerregister zu gewähren, sofern eine rechtliche Bestimmung Inhalt, Umfang und Modalitäten der Bekanntgabe regelt. Handelt es sich, wie im vorliegenden Fall, um einen leichteren Eingriff in die Freiheitsrechte, genügt eine Regelung in einem Erlass unterhalb der Gesetzesstufe. Das Abrufverfahren sowie die berechtigte Behörde und der Umfang der abrufbaren Daten sind darin ausdrücklich zu erwähnen.

Data-Mining-Projekt

Auch in der öffentlichen Verwaltung besteht zunehmend der Wunsch, aus gesammelten Personendaten zusätzlichen Nutzen zu ziehen. Beim Data Mining werden grössere Datenbestände neu kombiniert oder mit zusätzlichen Personendaten verknüpft und in einer separaten Datenbank zu Analysezwecken bearbeitet. So lassen sich neue Erkenntnisse über Personen gewinnen. Solche Projekte haben eine hohe Relevanz in Bezug auf die datenschutzrechtlichen Grundprinzipien. Sie müssen die Erfordernisse einer genügenden gesetzlichen Grundlage, der Zweckbindung, der Verhältnismässigkeit und der Transparenz einhalten. Der Datenschutzbeauftragte kam in seiner Vorabkontrolle zum Schluss, die geplante Datenbearbeitung sei für die betroffenen Personen zu wenig transparent. Er wies auch darauf hin, dass ein öffentliches Organ für den Umgang mit Informationen verantwortlich bleibt, auch wenn es eine Datenbearbeitung Dritten überträgt. Insbesondere muss das öffentliche Organ umfassend Kenntnis und Kontrolle über die Bearbeitung seiner zur Verfügung gestellten Personendaten haben und mit dem externen Dienstleister in einem Vertrag die wesentlichen Punkte der Datenbearbeitung festhalten. Das betroffene öffentliche Organ nahm in einer Nachbearbeitung des Projektes die Kritikpunkte auf.

§ 10 IDG, § 24 Abs. 1 lit. a und e IDV, § 38a Abs. 1 Gemeindegesetz, § 12 IDG, § 6 IDG, § 25 IDV

Auslagerung der Bearbeitung von Patientendaten

Im Gesundheitsbereich sind bei Datenbearbeitungen durch Dritte neben den datenschutzrechtlichen Voraussetzungen sowohl das Amts- als auch das Berufsgeheimnis zu beachten. Dies gilt auch dann, wenn es sich bei der Drittinstitution um ein anderes öffentliches Organ handelt. Der Auftrag setzt einen schriftlichen Vertrag voraus. Das Berufsgeheimnis wird nicht verletzt, wenn die Person, welche die Daten bearbeitet, als Hilfsperson qualifiziert werden kann sowie die Einwilligung der Betroffenen oder die Entbindung von der Aufsichtsbehörde vorliegt.

Spitäler gehen immer häufiger dazu über, Datenbearbeitungen nicht mehr selbst, sondern durch Dritte vornehmen zu lassen, sei dies aus Gründen der Effizienz oder der Spezialisierung. Betroffen davon sind beispielsweise die Auslagerung des Inkassos von Honorarforderungen oder Informatikdienstleistungen, wie Wartungsarbeiten an technischen Geräten. Werden solche besondere Personendaten durch externe Dienstleister, worunter auch sich vom Auftraggeber unterscheidende öffentliche Organe fallen, im Auftragsverhältnis bearbeitet, müssen nicht nur die datenschutzrechtlichen Voraussetzungen in Bezug auf die vertragliche Vereinbarung beachtet werden, sondern insbesondere auch das Arzt- und Patientengeheimnis.

Der Auftrag muss in schriftlicher Form mit dem geforderten minimalen Inhalt vorliegen. Handelt es sich wie im vorliegenden Fall um besondere Personendaten, ist der Vertrag zusätzlich von der vorgesetzten Stelle zu genehmigen.

Berufsgeheimnis erfordert zusätzliche Vorkehrungen

Während das Amtsgeheimnis einer Datenbearbeitung durch andere Organe grundsätzlich nicht entgegensteht, sind der Auslagerung von Datenbearbeitungen, die dem Berufsgeheimnis unterliegen, engere Grenzen gesetzt. Eine zentrale Rolle spielt dabei die Auslegung des Begriffs der Hilfsperson im Sinne des Strafgesetzbuches. Drei Vorgehensweisen stehen dabei zur Auswahl: Die erste Möglichkeit besteht darin, die Einwilligung der Betroffenen einzuholen. Dies kann mittels eines Formulars oder eines Zusatzes auf einem Formular vorgängig erfolgen, wobei der Zweck der Auslagerung, der Umfang sowie die Empfänger der Daten ersichtlich sein müssen. Zweitens können die mit der Datenbearbeitung betrauten Mitarbeitenden des Auftragnehmers in die funktionale Hierarchie des Auftraggebers eingebunden werden. Dies geschieht dadurch, dass einzelne Mitarbeiterinnen und Mitarbeiter für die Datenbearbeitung explizit bestimmt und schriftlich zur Einhaltung der Schweigepflicht verpflichtet werden sowie den Weisungen des Auftraggebers unterliegen. In diesem Fall werden sie als Hilfsperson qualifiziert. Schliesslich kann im Einzelfall bei der Aufsichtsbehörde – der Gesundheitsdirektion – die Entbindung von der Schweigepflicht eingeholt werden.

§ 25 IDV

Art. 321 Ziff. 1 Strafgesetzbuch

Art. 321 Strafgesetzbuch

Art. 321 Ziff. 2 Strafgesetzbuch

Videoüberwachung: Regelungsmöglichkeiten für Gemeinden

Seit einigen Jahren setzen die Gemeinden vermehrt Videoüberwachung ein. Dieser Eingriff in die Privatsphäre der Bürgerinnen und Bürger ist nur zulässig, wenn die allgemeinen Grundsätze des Datenschutzrechts sowie die besonderen Voraussetzungen zur Bearbeitung von Personendaten eingehalten werden. Der Datenschutzbeauftragte unterstützt die Gemeinden bei der Umsetzung des geltenden Rechts und stellt ihnen einen Leitfaden sowie ein Musterreglement für die Videoüberwachung zur Verfügung.

Werden Personen mittels Videoaufzeichnung überwacht, handelt es sich um eine Bearbeitung von Personendaten im Sinne des Datenschutzrechts. Diese ist zulässig, sofern sie sich auf eine rechtliche Grundlage abstützt oder sich aus den gesetzlich umschriebenen Aufgaben eines öffentlichen Organs ableiten lässt.

Unter den Begriff «Gemeinden» fallen die politischen Gemeinden, die Schulgemeinden sowie die Kirchgemeinden. Politische Gemeinden und Schulgemeinden können sich einzeln oder als Einheitsgemeinden organisieren. Die Kirchgemeinden sind stets unabhängig organisiert.

Zu den Aufgaben der politischen Gemeinde gehören die Aufrechterhaltung der öffentlichen Ruhe und Ordnung sowie der Schutz von Personen und Eigentum gegen Schädigung und Gefahren. Wenn es zur Erfüllung dieser Aufgabe geeignet und erforderlich ist, können die Gemeinden eine Videoüberwachung einsetzen. Gleiches gilt für die Schulgemeinden, die für die Aufrechterhaltung eines geordneten Schulbetriebs verantwortlich sind und dazu die geeigneten Massnahmen ergreifen dürfen. Gemäss Kirchengesetz sind die Vorschriften des Gemeindegesetzes auf die Kirchgemeinden sinngemäss anwendbar. Eine Videoüberwachung muss für die betroffenen Personen erkennbar sein. Das datenschutzrechtliche Transparenzprinzip verlangt eine rasche, umfassende und sachliche Information. Der Datenschutzbeauftragte empfiehlt den Gemeinden dabei, eine der folgenden Varianten zu wählen:

Erlass eines Reglements, das die Einzelheiten der Videoüberwachung festlegt, oder eine einheitliche Regelung der Videoüberwachung mehrerer Gemeindebehörden auf Gesetzesstufe.

Reglement zur Videoüberwachung

Die verschiedenen Gemeindebehörden können jeweils ein Reglement zu den einzelnen Überwachungsanlagen erlassen. Daraus muss für die betroffenen Bürgerinnen und Bürger ersichtlich sein, wo und zu welchen Tageszeiten sie mittels Videoaufzeichnungen überwacht werden sowie welches Organ für die Bearbeitung und Auswertung der Aufzeichnungen verantwortlich ist. Zudem soll das Reglement Angaben zur Aufbewahrungsdauer und zur Löschung der Aufzeichnungen sowie zu den Massnahmen zur Gewährleistung der Datensicherheit (Ort der Aufbewahrung, Protokollierung der Zugriffe etc.) enthalten. Empfehlenswert ist auch die Bezeichnung einer zuständigen Stelle oder einer Ansprechperson, an welche sich betroffene Personen wenden können.

Werden in einer Gemeinde mehrere Standorte mittels Videoaufzeichnung überwacht, können diese – unter Angabe der Standorte und der Betriebsdauer der einzelnen Kameras – auch in einem einzigen Reglement zusammengefasst werden. Ein solches Reglement kann durch den Gemeinderat oder auch die zuständigen Organe der Schul- und Kirchgemeinden erlassen werden.

Gesetz zur Videoüberwachung

Politische Gemeinden können die genannten Angaben zur Videoüberwachung auch auf Gesetzesstufe regeln, also mit Zustimmung der Gemeindeversammlung. Da sich die Standorte oder die jeweilige Betriebsdauer der Überwachungsanlagen jedoch ändern können, müssen diese auch innert nützlicher Frist angepasst werden können. Deshalb empfiehlt es sich, diese Details in einem Zusatzreglement festzuhalten, das bei Bedarf durch den Gemeinderat ergänzt oder abgeändert werden kann und nicht der Genehmigung durch die Gemeindeversammlung bedarf. Dabei bleibt es den Gemeinden überlassen, wie detailliert die gesetzliche Grundlage beziehungsweise das Zusatzreglement ausgestaltet wird. Möglich ist ein ausführliches Kurzreglement zu jeder Überwachungsanlage oder eine einfache Liste, die lediglich den Standort und die Betriebsdauer der einzelnen Anlagen enthält.

Einführung einer Bewilligungspflicht bei Einheitsgemeinden

In einer Einheitsgemeinde kann die Einrichtung einer Videoüberwachungsanlage durch die Gemeindeorgane einer Bewilligungspflicht durch den Gemeinderat unterstellt werden. Dieser kann die Verhältnismässigkeit der Überwachungsanlage prüfen und durch eine weniger einschneidende Massnahme ersetzen, sofern diese den gleichen Zweck erfüllt. So kann ein unverhältnismässiger Einsatz von Videoüberwachungsanlagen in der Gemeinde verhindert werden.

Aufzeichnung von Straftaten

Die Kompetenz zur Verfolgung von Straftaten liegt ausschliesslich bei den gesetzlich bestimmten Strafverfolgungsorganen. Werden bei einer Videoüberwachung strafrechtlich relevante Handlungen registriert, sind die Aufzeichnungen unverzüglich den zuständigen Behörden zu übergeben.

§ 4 IDG

§ 8 Abs. 1 IDG

§ 12 IDG

§ 74 Gemeindegesetz

Weitergabe von IV-Rentenentscheiden

Die IV-Stelle ist an die Schweigepflicht gebunden. Gegenüber einer im Gesetz nicht genannten Behörde darf sie einen IV-Rentenentscheid nur herausgeben, wenn die betroffene Person in die Datenbekanntgabe einwilligt.

Im Rahmen eines Rekurses betreffend eine Niederlassungsbewilligung ersuchte die Rekursbehörde die zuständige IV-Stelle, ihr eine Kopie eines IV-Rentenentscheids zu überlassen. Die IV-Stelle wandte sich daraufhin an den Datenschutzbeauftragten, um zu prüfen, ob diese Datenbekanntgabe rechtmässig ist.

Sozialversicherungsrechtliche Schweigepflicht

Auf den zu beurteilenden Sachverhalt ist das Sozialversicherungsrecht des Bundes anwendbar. Dieses sieht für die IV-Stellen eine Schweigepflicht vor, von der nur abgewichen werden darf, wenn das Gesetz dies ausdrücklich zulässt. Das hier anwendbare AHV-Gesetz enthält eine Liste von Fällen, in denen eine Datenbekanntgabe erlaubt ist. Darin vorgesehen sind zum Beispiel Mitteilungen an Steuerbehörden oder Strafgerichte, nicht jedoch an kantonalen Rekursbehörden. Eine Datenbekanntgabe gegenüber einer Rekursbehörde ist nur möglich, wenn die betroffene Person im Einzelfall schriftlich einwilligt.

Die Rekursbehörde begründete ihre Anfrage mit einer Bestimmung im kantonalen Verwaltungsrechtspflegegesetz, wonach Verwaltungsbehörden und Gerichte verpflichtet sind, für die Sachverhaltsfeststellung notwendige Akten herauszugeben. Besondere Vorschriften über die Geheimhaltung und den Datenschutz bleiben gemäss Verwaltungsrechtspflegegesetz vorbehalten. Diese Amtshilfebestimmung vermag die Schweigepflicht der IV-Stelle nicht aufzuheben: Erstens geht das Bundesrecht dem kantonalen Recht vor, so dass die bundesrechtliche Schweigepflicht durch die kantonale Bestimmung über die Aktenherausgabe nicht aufgehoben wird. Die Schweigepflicht und ihre Ausnahmen sind im Bundesrecht abschliessend geregelt. Zweitens steht die Bestimmung über die Aktenherausgabe selber unter dem Vorbehalt besonderer Vorschriften über die Geheimhaltung und den Datenschutz. Selbst wenn sie also anwendbar wäre, bliebe die Schweigepflicht der IV-Stelle bestehen.

Ausländerrechtliche Amtshilfebestimmung

Die Schweigepflicht der IV-Stelle ergibt sich aus dem Sozialversicherungsrecht. Offen ist die Frage, ob die Schweigepflicht durch bundesrechtliche Amtshilfebestimmungen ausserhalb des Sozialversicherungsrechts durchbrochen werden kann. Dies erscheint nicht zulässig, weil Ausnahmen von der Schweigepflicht üblicherweise im Gesetz selber aufgelistet werden. So wurde die Datenbekanntgabe im AHV-Gesetz ausdrücklich geregelt, als der Bund ein Gesetz zur Bekämpfung der Schwarzarbeit erliess. Im vorliegenden Fall existiert eine Amtshilfebestimmung im Bundesgesetz über die Ausländerinnen und Ausländer. Es fehlt jedoch eine entsprechende Analogie im AHV-Gesetz. Zudem ist die Amtshilfebestimmung sehr allgemein formuliert und zu wenig bestimmt, um die Schweigepflicht zu durchbrechen. Vor diesem Hintergrund ist deshalb eine Datenbekanntgabe nur mit schriftlicher Einwilligung der betroffenen Person möglich.

§ 7 Abs. 3 Verwaltungsrechtspflegegesetz

Art. 33 Allgemeiner Teil des Sozialversicherungsrechts

Art. 50a AHV-Gesetz i.V.m. Art. 66a IV-Gesetz

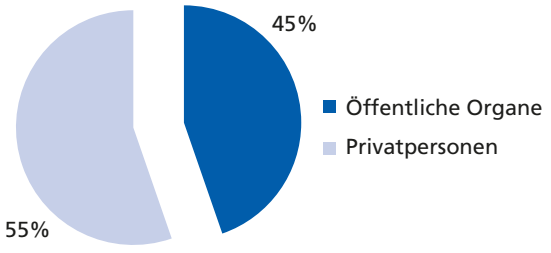
Art. 49 Abs. 1 Bundesverfassung

Beratung von Privatpersonen

Zu wissen, welche Behörde Daten über die eigene Person bearbeitet, welche Rechte diesbezüglich ausgeübt werden können und ob die Daten rechtmässig bekannt gegeben werden – das sind die Fragen, die Privatpersonen immer wieder interessieren. Anfragen zu Datenpublikationen im Internet und deren Löschung bildeten 2010 einen Schwerpunkt.

Jede Person, die sich mit einem datenschutzrechtlichen Anliegen an den Datenschutzbeauftragten wendet, wird beraten. Sei dies, dass eine massgeschneiderte Lösung direkt mündlich erarbeitet oder die Person an das zuständige öffentliche Organ verwiesen wird; sei es, dass weitere schriftliche Abklärungen getätigt werden. Dabei wird jeder Einzelfall analysiert, im Gesamtkontext begutachtet und in Zusammenarbeit mit den betroffenen Behörden gelöst. Für 2010 kann festgestellt werden, dass die Beratung von Privatpersonen rund 55% der telefonischen Beratungstätigkeit des Datenschutzbeauftragten umfasste und mehrere hundert Anfragen bearbeitet wurden.

Telefonische Kurzberatungen 2010



Oftmals sind es die kleinen Schritte einer Datenbearbeitung, die grosses Potenzial im Hinblick auf Persönlichkeitsverletzungen aufweisen, wie beispielsweise die Veröffentlichung von Daten im Internet. Die Gesetze sind in vielen Fällen zu unbestimmt und enthalten oftmals keine ausreichenden Regelungen, um eine datenschutzkonforme Bearbeitung zu garantieren.

Was Bürgerinnen und Bürger beschäftigt

Die im Berichtsjahr bearbeiteten Themen waren erneut breit gefächert und reichten von Datenbearbeitungen mit Bezug zum Arbeitsrecht über das Bearbeiten medizinischer Daten bis hin zu Fragen betreffend die Datenerfassung zwecks Registerharmonisierung. Ein Grossteil der Anfragen betraf das von Privatpersonen in Anspruch genommene Auskunftsrecht. Oftmals wurde die Einsicht von den zuständigen Behörden verweigert, oder eine Ablehnung wurde nicht rechtmässig mit einer Verfügung und Rechtsmittelbelehrung mitgeteilt. Auch die Kostenfrage bei der Anfertigung von Kopien spielte immer wieder eine Rolle. Der Datenschutzbeauftragte intervenierte in diesen Fällen bei den entsprechenden öffentlichen Organen und verhalf so den Betroffenen zur Durchsetzung ihrer Rechte.

Einen weiteren Schwerpunkt bildeten Anfragen zur Publikation von Daten im Internet. Dabei handelte es sich um Lebensläufe, Fotos, aber auch um Personendaten wie Name, Adresse oder Telefonnummer. Die Gesetze schweigen sich diesbezüglich in den meisten Fällen aus. Es ist daher unerlässlich, jede einzelne Publikation auf ihre Verhältnismässigkeit hin zu überprüfen. Informationen im Internet sind unkontrollierbar, von jedermann einsehbar und nur unter erschwerten Umständen – wenn überhaupt – zu löschen. Im Berichtsjahr registrierte der Datenschutzbeauftragte auch zahlreiche Anfragen zu den neuen Bestimmungen für die auf harmonisierten Registern basierende Volkszählung. Sie führte dazu, dass Behörden eine Vielzahl von Personendaten zu erfassen hatten, hierfür aber über keine ausreichende gesetzliche Grundlagen verfügten. Absenzeinträge in Zeugnissen sowie Datenbekanntgaben durch Schulen bei Impfkampagnen waren weitere Themen, die der Datenschutzbeauftragte 2010 im Rahmen seiner Beratungen für Privatpersonen bearbeitete.

Angaben in der Erziehungsverfügung

Der Jugendanwalt schliesst eine Untersuchung in der Regel mit einer Erziehungsverfügung ab. Gemäss Zürcher Strafprozessordnung wird die Verfügung dem Angeschuldigten, der Jugendstaatsanwaltschaft, den gesetzlichen Vertretern und dem Opfer schriftlich zugestellt. Weitere Geschädigte erhalten den Entscheid im Dispositiv. Geschädigte erhalten so auch von denjenigen Delikten des Angeschuldigten Kenntnis, von denen sie selber nicht betroffen sind. Mit Inkrafttreten der Schweizerischen Jugendstrafprozessordnung werden Geschädigte nur noch insoweit informiert, als ihre Anträge behandelt werden.

Die Jugendanwaltschaft schloss ein von ihr eröffnetes Jugendstrafverfahren gegen einen mehrfachen Delinquenten mittels Erziehungsverfügung ab und versandte das Dispositiv des Strafbefehls an alle Geschädigten sowie deren gesetzliche Vertreter. Dem Rechtsvertreter des Jugendlichen erschien diese Mitteilungspraxis völlig unverhältnismässig. In seinem Schreiben an den Datenschutzbeauftragten kritisierte er, dass von den insgesamt neun im Urteilsdispositiv aufgelisteten strafrechtlichen Vorwürfen längst nicht alle Geschädigten gleichermassen betroffen seien. So habe ein Geschädigter, der einzig vom Tatbestand der falschen Anschuldigung berührt gewesen sei, auch vom mehrfach begangenen Raub und weiteren Delikten des Angeschuldigten erfahren. Ziehe man in Betracht, in welch engem sozialem Umfeld sich die heutige Jugendkriminalität abspiele, entspreche diese Form von Mitteilung einem Pranger. Der betroffene Jugendliche müsse jedoch weiterhin die Schule besuchen und sich um eine Lehrstelle bemühen.

Unbefriedigende Mitteilungspraxis

Informationen über Personen, die strafrechtlich verfolgt werden, sind besondere Personendaten. Für deren Bekanntgabe ist eine hinreichend bestimmte Regelung in einem formellen Gesetz notwendig. Die Zustellung von Erziehungsverfügungen bei Verfahren gegen Jugendliche ist in der Zürcher Strafprozessordnung geregelt. Demgemäss erhalten Geschädigte das Dispositiv des Entscheids und auf Verlangen auch die Begründung bezüglich zivilrechtlicher Ansprüche.

Die Jugendstaatsanwaltschaft zeigte in ihrer Stellungnahme Verständnis dafür, dass die gesetzlichen Vorgaben von einem betroffenen Jugendlichen im Einzelfall als stossend empfunden werden können. Deshalb werde über Verfahrenseinstellungen in der Regel separat verfügt, so dass ein Geschädigter nur über die ihn betreffende Sache Kenntnis erhalte. Ein Verfahren mit Erziehungsverfügung müsse aber als Ganzes abgeschlossen werden. Das Dispositiv könne auch deshalb nicht auseinanderdividiert werden, weil die daraus hervorgehende ausgefällte und möglicherweise hohe Strafe für den einzelnen Geschädigten nicht nachvollziehbar sei, wenn sie nur einem einzelnen geringfügigen Delikt gegenüberstünde.

Mehr Persönlichkeitsschutz in der neuen Jugendstrafprozessordnung

Die Schweizerische Jugendstrafprozessordnung, die am 1. Januar 2011 in Kraft getreten ist, trägt dem Persönlichkeitsschutz mehr Rechnung. Die entsprechende Bestimmung hält fest, dass der Strafbefehl dem Geschädigten nur in dem Umfang eröffnet wird, als seine Anträge behandelt werden. Damit wird auch die speziell für Jugendliche vorgesehene Bestimmung bezüglich Nichtöffentlichkeit des Verfahrens umgesetzt.

§ 384 Abs. 4 Strafprozessordnung Kanton Zürich

Art. 32 Abs. 4 lit. b Jugendstrafprozessordnung

Art. 14 und 15 Jugendstrafprozessordnung

Einbürgerungsdaten im Internet

Im Verlauf einer Einbürgerung auf Gemeindeebene werden Personendaten über verschiedene Medien veröffentlicht. Publikationen im Internet weisen damit ein hohes Risiko einer Persönlichkeitsverletzung auf. Die Daten sind einem unbegrenzten Personenkreis zugänglich, auf lange Zeit unkontrolliert abrufbar und nur unter erschwerten Bedingungen, wenn überhaupt, zu löschen. Es muss deshalb stets geprüft werden, ob eine Veröffentlichung über das Internet verhältnismässig ist und, wenn ja, dass nur die für die Identifikation notwendigen Daten veröffentlicht werden wie Name, Vorname, Geschlecht, Geburtsjahr und Staatsangehörigkeit.

Eine Bürgerin war vor mehreren Jahren in einer Zürcher Gemeinde eingebürgert worden. Das damalige Weisungsheft für die Gemeindeversammlung mit ihren persönlichen Daten ist immer noch auf der Gemeinde-Website aufgeschaltet und erscheint bei einer Google-Suche nach ihrem Namen ganz oben auf der Trefferliste.

Während eines Einbürgerungsverfahrens auf Gemeindeebene werden verschiedene Personendaten der betroffenen Personen in verschiedenen Medien veröffentlicht. Es handelt sich dabei insbesondere um Name, Vorname, Geschlecht, Geburtsjahr, Staatsangehörigkeit, Adresse, Wohnsitzdauer, Zivilstand, Ausbildung, Antrag der Einbürgerungskommission und weitere Personendaten wie zum Beispiel Wohnorte und Wohndauern vor dem Einbürgerungsgesuch, Beruf, aktuelle und ehemalige Arbeitsstellen oder die Beziehung zum Herkunftsland.

Die Veröffentlichung dieser Daten erfolgt hauptsächlich im amtlichen Publikationsorgan, dem Weisungsheft, durch Aktenauflage in der Gemeindekanzlei oder im Internet. Bei einer Internetpublikation werden die Personendaten entweder direkt auf der Gemeinde-Website oder durch Aufschalten des amtlichen Publikationsorgans oder des Weisungsheftes veröffentlicht.

Spärliche rechtliche Voraussetzungen

Eine Datenbekanntgabe ist grundsätzlich gestützt auf eine hinreichend bestimmte Rechtsgrundlage oder die Einwilligung der betroffenen Person zulässig. Rechtsgrundlagen für die Veröffentlichung bestimmter Daten im Zusammenhang mit Einbürgerungsverfahren finden sich in der kantonalen Bürgerrechtsverordnung, dem Gemeindegesetz sowie dem Bürgerrechtsgesetz des Bundes. Alle äussern sich aber nur in geringem Ausmass oder gar nicht zu den Datenkategorien und Publikationsmitteln. Das Einreichen eines Einbürgerungsgesuches ist keine Einwilligung in die Publikation der persönlichen Daten im Internet.

Um Persönlichkeitsverletzungen zu vermeiden, muss das Verhältnismässigkeitsprinzip beachtet werden. Es müssen sämtliche Datenkategorien und Publikationsmittel einzeln dahin gehend überprüft werden, ob sie im Zusammenhang mit einer Einbürgerung geeignet und erforderlich sind. Im Internet sind nur die für die Identifikation einer Person notwendigen Daten zu veröffentlichen wie Name, Vorname, Geschlecht, Geburtsjahr und Staatsangehörigkeit.

Im vorliegenden Fall erwies sich die bestehende (veraltete) Publikation als unverhältnismässig, und die Gemeinde war bereit, die entsprechenden Daten zu löschen.

§§ 16 Abs. 1 und 17 Abs. 1 IDG

§§ 13 Abs. 4 und 17 Bürgerrechtsverordnung

§§ 43 Abs. 1 und 100 Gemeindegesetz

Art. 15c Bürgerrechtsgesetz

Mehr Informationssicherheit durch Know-how-Transfer

Die rasante Entwicklung der Informationstechnologie sowie die stetig wachsenden Datenmengen erfordern regelmässige, schwerpunktmässige und sachbezogene Prüfungen der rechtlichen, organisatorischen und technischen Rahmenbedingungen der Datenbearbeitungen einer Verwaltungsstelle. Verbunden mit der Vermittlung von Know-how und einer Beratung bietet dies die bestmögliche Gewähr für einen minimalen Standard im Bereich der Informationssicherheit.

Im Berichtsjahr fokussierte der Datenschutzbeauftragte auf die Überprüfung von Bearbeitungen besonderer Personendaten und den Transfer von Fachwissen. Bei den durchgeführten Kontrollen kristallisierten sich zwei Schwachpunkte heraus: Es zeigte sich, dass nicht nur mangelnde Ressourcen Ursache fehlender Massnahmen im Bereich der Informationssicherheit sind, sondern auch Unsicherheit in Bezug auf den vom Gesetz geforderten Standard sowie mangelndes Know-how. Mehrheitlich stellte der Datenschutzbeauftragte das Fehlen von Sicherheitsleitlinien und -konzepten oder von Rollen- und Berechtigungskonzepten fest.

Kontrolle der Bearbeitung besonderer Personendaten

2010 überprüfte der Datenschutzbeauftragte die Datenbearbeitungen in Spitälern und bei der Kantonspolizei sowie in den Bereichen Strafvollzug und E-Government. Hauptsächlich wurde das Fehlen von Sicherheitsstrategien und -leitlinien, von Vorgaben an Dienstleistende bei Auslagerungen, von Richtlinien für die Bereiche des Incident- und Problemmanagements sowie von Rollen- und Berechtigungskonzepten bemängelt. Die Resultate der Prüfungen erforderten keine Empfehlung durch den Datenschutzbeauftragten; die Hinweise und die vorgeschlagenen Massnahmen ermöglichen es den geprüften Stellen aber, den Sicherheitsstandard weiter zu verbessern.

Vermittlung von Wissen

Zur Unterstützung der Informatikverantwortlichen der Gemeinden bot der Datenschutzbeauftragte im Berichtsjahr erstmals regelmässig Kurse zum Thema Informationssicherheit an. Im Rahmen der Schulung erwarben die Teilnehmerinnen und Teilnehmer die Grundlagen, um die notwendigen Massnahmen zur Informationssicherheit umzusetzen.

Weiter wurde die Erarbeitung einer Dokumentation zur Informationssicherheit anhand einer Pilotgemeinde an die Hand genommen.

Datenschutzrechtliche Kontrolle beim Staatsschutz

Der Datenschutzbeauftragte überprüfte im Berichtsjahr die Datenbearbeitungen der Kantonspolizei im Bereich des Staatsschutzes. Nach anfänglicher Verzögerung wurde die Kontrolle mittels Stichproben und unter Teilnahme von Vertretern des Bundes durchgeführt. Kernpunkte waren die Überprüfung der Verwaltungsabläufe mit Blick auf die geltenden eidgenössischen und kantonalen Gesetzesbestimmungen sowie das Einhalten der erforderlichen Massnahmen im Bereich der Informationssicherheit.

Die kantonalen Vollzugsbehörden im Bereich des Staatsschutzes sind im Kanton Zürich die Kantons- und die Stadtpolizei. Im Jahr 2009 wurde eine datenschutzrechtliche Kontrolle bei der Kantonspolizei eingeleitet, die im Berichtsjahr ihren Abschluss fand. Die unüblich lange Dauer war auf unterschiedliche Rechtsauffassungen und die sich daraus ableitenden anfänglichen Weigerung einer Kontrolle vor Ort durch die Kantonspolizei zurückzuführen. Der Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte zu dieser Thematik sowie weitere Diskussionen im Hinblick auf die Regelung der Aufsicht im Bereich des Staatsschutzes führten schliesslich dazu, dass die Prüfung durchgeführt werden konnte. Aufgrund der komplexen Ausgangslage fand die Kontrolle nicht wie üblich vollständig unabhängig statt, sondern die Einsicht in die Daten konnte nur mit Zustimmung sowie in Anwesenheit von Vertretern des Nachrichtendienstes des Bundes erfolgen und beschränkte sich auf Stichproben. Nicht überprüft wurden die Datenbeschaffung und die weitere Datenbearbeitung im Hinblick auf die Verhältnismässigkeit. Sollten die Voraussetzungen für eine umfassende unabhängige Kontrolltätigkeit geschaffen werden, wird der Datenschutzbeauftragte zu einem späteren Zeitpunkt eine vollumfängliche Kontrolle in Erwägung ziehen.

Komplexes Prüfungsumfeld

Die Datenbearbeitung im Bereich des Staatsschutzes erfolgt durch die Kantonspolizei in enger Zusammenarbeit mit den Bundesbehörden, die auch die entsprechenden Aufträge erteilen. Die bearbeiteten Daten werden nach der Erhebung und Bearbeitung an den Bund weitergeleitet oder vernichtet. Ein Duplikat der Daten verbleibt bei der Kantonspolizei und unterliegt als solches der kantonalen datenschutzrechtlichen Aufsicht. Als Erstes überprüfte der Datenschutzbeauftragte die vom Gesetz festgehaltenen Verwaltungsabläufe inklusive des Löschungsverfahrens. Konkret bedeutete dies, das Erheben, Bearbeiten und Weiterleiten der Daten mit Blick auf den Auftrag oder die eigenen Erkenntnisse zu analysieren, den Ermessensspielraum herauszufiltern und diesen mit den geltenden gesetzlichen Bestimmungen abzugleichen. Neben der Überprüfung der sicheren Aufbewahrung und der Einhaltung der Löschungsfristen kontrollierte der Datenschutzbeauftragte auch, ob die Richtigkeit und die Verhältnismässigkeit der Datenbearbeitungen durch die Vorgesetzten ausreichend geprüft wurden. Als weiterer Schwerpunkt wurden die im Bereich der Informationssicherheit umgesetzten organisatorischen und technischen Massnahmen kontrolliert. Dabei wurde unter anderem geprüft, ob Zugriffe von Unberechtigten protokolliert, Löschungen dokumentiert, Rollenkonzepte erstellt und Massnahmen umgesetzt worden waren.

Der Prüfungsbericht enthält zahlreiche Hinweise und Bemerkungen betreffend die rechtlichen Aspekte sowie die organisatorischen und technischen Massnahmen der Datenbearbeitungen. Mängel, die zu sofortigem Handeln Anlass gegeben hätten, wurden nicht festgestellt.

Vertraulichkeit des E-Governments-Angebots geprüft

Der Datenschutzbeauftragte prüfte im Berichtsjahr die Vertraulichkeit der übertragenen Daten in der neuen E-Government-Plattform ZHservices. Das komplexe Informatikumfeld mit seinen zahlreichen Akteuren erfordert differenzierte Instrumente zur Gewährleistung der Vertraulichkeit. Nachdem zahlreiche Massnahmen bereits getroffen wurden, werden die Hinweise des Datenschutzbeauftragten Betrieb und Entwicklung von ZHservices weiter optimieren.

Der Kanton Zürich erweiterte 2010 sein Transaktionsangebot im Bereich E-Government auf der Plattform ZHservices: Neu können Armee- und Zivilschutzangehörige Dienstverschiebungsgesuche und Gesuche um Auslandurlaub über das Internet einreichen.

Organisatorische und technische Massnahmen im Fokus

Ziel der Prüfung des Datenschutzbeauftragten war es, die organisatorischen und technischen Massnahmen für den elektronischen Amtsverkehrs einer vertieften Prüfung zu unterziehen. Beurteilt wurde, ob der gesamte Informationsfluss von der Dateneingabe in der Browsermaske bis zur Verarbeitung in der Fachapplikation nur für die Beteiligten einsehbar ist. Mittels Interviews und Stichproben in den Hauptpunkten Datenfluss, Betriebsabläufe, Zugriffsvergabe und Sicherheitsmanagement sowie mittels Vergleich der bestehenden Dokumentation mit den eingerichteten Prozessen wurden die zahlreichen Informatikkomponenten bei den verschiedenen Dienstleistenden für ZHservices vor Ort unter die Lupe genommen. Die mit den einzelnen Dienstleistenden und Kunden getroffenen Vereinbarungen wurden ebenfalls begutachtet.

Aufschlussreiches Prüfungsresultat

Feststellungen und Hinweise betrafen die folgenden Bereiche:

Sicherheitsmanagement: Das fehlende Sicherheitsumfeld behindert zurzeit insbesondere im organisatorischen Bereich eine Durchsetzung der notwendigen Massnahmen. Die Schaffung von angemessenen Grundlagen und der Aufbau eines Sicherheitsmanagementsystems müssen prioritär in Angriff genommen werden.

Vertragsmanagement: In den Verträgen fehlten teilweise Vorgaben wie Anforderungen an die Informatiksicherheit, Massnahmen zum Nachweis von Korrektheit und Funktionalität der Lösung bei Nachbesserung und Erweiterung, Abnahmekriterien sowie Rapport- oder Kontrollmechanismen.

Entwicklung von ZHservices: Obwohl der Projektabschluss dokumentiert wurde, fehlten für die Erweiterungen und Änderungen die notwendigen Abnahmeprozeduren mit den entsprechenden Kriterien. Diese Arbeiten müssen einer zu schaffenden Rolle eines Betriebsverantwortlichen zugewiesen werden.

Betrieb von ZHservices: Die Vertraulichkeit kann durch die Änderung von bestimmten Transportkomponenten optimiert werden. Es ist die Rolle eines Betriebsverantwortlichen, mit der ausreichenden Zuweisung von personellen und finanziellen Mitteln für genügend Transparenz zu sorgen. Teilweise fehlende Betriebsprozesse und die Überwachung der zahlreichen Teilkomponenten in einer Gesamtschau müssen ebenfalls noch eingerichtet werden.

Kontrolle: Weitere Prüfungen insbesondere im SAP-Umfeld und im Sicherheitsumfeld sind noch zu planen.

Einfluss auf andere Informatikprojekte

Mit dieser Prüfung zeigte der Datenschutzbeauftragte notwenige Korrekturen auf. Die Amtsstelle hat die dringendsten Probleme bereits angepackt und eine Grobplanung für weitere Massnahmen erstellt. Besonders auch für die neuen Anwendungen, die sich, wie beispielsweise die Online-Steuererklärung, auf ZHservices stützen werden, konnte die Prüfung wichtige Impulse im Bereich Informatiksicherheit vermitteln.

Auslagerung von Informatiksystemen

Bei der Auslagerung von Informatikdienstleistungen ist eine vertragliche Vereinbarung zu treffen, die die Verantwortlichkeiten des öffentlichen Organs sowie des Dienstleisters klar regelt und das Personal des Dienstleisters den gesetzlichen Geheimhaltungspflichten wie Amts- und Berufsgeheimnis unterstellt. Die Vereinbarung betreffend den Betrieb eines SAP-Systems für das Rechnungswesen wurde von der Finanzdirektion in verschiedenen Punkten entscheidend nachgebessert.

Für das Rechnungswesen verwenden die Zentralverwaltung, die psychiatrischen Kliniken und das Universitätsspital schon seit einigen Jahren die Software SAP. Der Betrieb der Systeme war an verschiedene Dienstleister ausgelagert. Der Regierungsrat entschied nach einer öffentlichen Ausschreibung, den Betrieb des Rechnungswesens mit SAP bei einem zentralen Dienstleister zusammenzufassen. Werden Informatikdienstleistungen von einem Dritten erbracht, kommen das Gesetz über die Auslagerung von Informatikdienstleistungen und das IDG zur Anwendung. Trotz Auslagerung bleibt die Verantwortung für die Informationsbearbeitungen beim öffentlichen Organ. Im vorliegenden Fall wurden im Rechnungswesen besondere Personendaten bearbeitet, weil Kliniken kostenpflichtige Leistungen inklusive Medikation über SAP abrechnen. Der Datenschutzbeauftragte liess deshalb der Finanzdirektion einen Fragekatalog zukommen, um abzuklären, ob die datenschutzrechtlichen Anforderungen eingehalten werden. Folgende Fragen wurden dabei gestellt:

– Wie sind die Verantwortlichkeiten zwischen dem öffentlichen Organ und dem Dienstleister vertraglich geregelt?
– Welche technischen und organisatorischen Massnahmen sind vorgesehen, damit die Datenbearbeitungen der einzelnen öffentlichen Organe getrennt erfolgen?
– Wie wird sichergestellt, dass beim Dienstleister intern nur diejenigen Personen Zugang zu den Daten erhalten, die dem Weisungs- und Kontrollrecht des öffentlichen Organs unterstellt und denen die jeweiligen Geheimnisregelungen (Amtsgeheimnis, medizinisches Berufsgeheimnis) überbunden wurden?

Anpassungen in wesentlichen Punkten

Ihrer Stellungnahme legte die Finanzdirektion die massgeblichen Unterlagen wie Muster-Geheimhaltungsvereinbarung, Rahmenvertrag für IT-Dienstleistungen sowie Entwurf eines Service-Level-Agreements bei. Basierend auf den Vorschlägen des Datenschutzbeauftragten wurde die Vereinbarung mit dem Dienstleister in folgenden Bereichen angepasst: Dem Dienstleister wurde die Verpflichtung auferlegt, sein für die SAP-Anwendung zuständiges Personal nicht nur dem Amtsgeheimnis, sondern auch dem medizinischen Berufsgeheimnis zu unterstellen. Die Geheimhaltungsverpflichtungen des Personals des Dienstleisters wurden verschärft und bleiben nach Austritt nicht nur während zweier Jahren sondern unbefristet bestehen. Für die technischen und organisatorischen Massnahmen wurden zudem in den Bereichen «Network Security Management», «Security Management» und «SAP User Management» klare Verantwortlichkeiten vereinbart. Der Dienstleister wurde ausserdem verpflichtet, Datenbestände wie Sicherheitskopien, Programme, Daten etc. zu vernichten, wenn sie nicht mehr benötigt werden, spätestens aber bei Vertragsende, und es wurde geregelt, dass sämtliche Datenbearbeitungen in der Schweiz erfolgen, damit sich keine weiteren Fragen betreffend grenzüberschreitende Datenbekanntgabe stellen. Die Finanzdirektion stellte des Weiteren in Aussicht, formellgesetzliche Grundlagen für das Kompentezzentrum SAP der Finanzdirektion zu schaffen, und sie hat ein entsprechendes Vorhaben ins Rechtssetzungsprogramm im Konsolidierten Entwicklungs- und Finanzplan (KEF) 2011–2014 aufgenommen.

§ 1 Abs. 3 Auslagerungsgesetz, § 3 Auslagerungsgesetz, § 6 IDG, § 7 IDG, § 25 IDV

Aktive Zusammenarbeit bewährt sich

Es gibt nur wenige Vollzugsaufgaben der Verwaltung, bei denen keine Personendaten bearbeitet werden. Deshalb weisen praktisch alle Gesetzgebungsvorhaben einen Bezug zum Datenschutz auf. Der Datenschutzbeauftragte kann schon bei der Erarbeitung der Gesetzesvorlage oder in der Vernehmlassung einbezogen werden.

Der moderne Rechtsstaat beruht auf dem Legalitätsprinzip. Das heisst, dass jegliches staatliches Handeln einer gesetzlichen Grundlage bedarf. Die Entwicklungen und Veränderungen in Gesellschaft, Wirtschaft und Technologie bringen es mit sich, dass immer wieder neue Gesetze erlassen und bestehende revidiert werden. Das Legalitätsprinzip gilt auch für das Bearbeiten von Personendaten. Will ein öffentliches Organ Informationen über Personen erheben, bearbeiten oder weitergeben, greift es in das Grundrecht auf Wahrung der Privatsphäre ein. Je sensibler die Informationen, desto höher muss die Legitimation für den Eingriff sein. Datenbearbeitungen benötigen deshalb gesetzliche Grundlagen. Das IDG als Rahmengesetz gibt vor, welche Art von Rechtsgrundlagen für welche Datenbearbeitungen erforderlich sind: Werden besondere Personendaten bearbeitet, wie beispielsweise solche, die Religion, Herkunft, Weltanschauung, Gesundheit, den Erhalt von Sozialhilfe oder strafrechtliche Sanktionen betreffen, muss dies in hinreichend bestimmter Form auf formellgesetzlicher Ebene geregelt sein. Das Bearbeiten von anderen Personendaten ist erlaubt, wenn dies zur Erfüllung der gesetzlichen Aufgaben des öffentlichen Organs – diese sind im Gesetz formuliert – geeignet und erforderlich ist.

Überlegungen bei Regulierungsprojekten

Bei Gesetzgebungsvorhaben ist zu prüfen, ob im Vollzug Daten bearbeitet werden. Dies kann in den allermeisten Fällen bejaht werden. Sodann ist die Überlegung anzustellen, ob die geplanten Rechtsgrundlagen dazu ausreichen. Massstab ist das IDG. Unter Umständen empfiehlt es sich, den Datenschutzbeauftragten schon in der Redaktions- oder der Konzeptphase zu konsultieren. Spätestens in der Vernehmlassung ist der Datenschutzbeauftragte einzubeziehen.

Der Datenschutzbeauftragte hat 2010 unter anderem zu folgenden Gesetzesprojekten Stellung bezogen:

Kanton

- Kantonsratsgesetz und Geschäftsreglement des Kantonsrates: Nachführung und Effizienzsteigerung
- Geoinformationsgesetz (Neuerlass)
- Sozialhilfegesetz
- Kinder- und Jugendhilfegesetz (Totalrevision)
- Pflegegesetz (Neuerlass)
- Spitalplanungs- und -finanzierungsgesetz (Neuerlass)
- Einführungsgesetz zum Krankenversicherungsgesetz
- Tierseuchengesetz (Totalrevision)
- Verordnung über psychiatrische Gutachten in Strafverfahren
- Grundbuchverordnung

Bund

- Bundesgesetz über die polizeilichen Aufgaben des Bundes (Neuerlass)
- Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (Totalrevision)
- Heilmittelgesetz
- Betäubungsmittelverordnungen
- Bürgerrechtsgesetz (Totalrevision)
- Zeugenschutzgesetz (Neuerlass)
- Alkoholgesetz (Totalrevision)

Neuordnung der Spital- und Pflegefinanzierung

Die Neuordnung der Spital- und Pflegefinanzierung beinhaltet auch den Austausch von zahlreichen sensiblen Gesundheitsdaten zwischen den verschiedenen verantwortlichen Organen. In seinen Stellungnahmen wies der Datenschutzbeauftragte auf das Erfordernis einer hinreichend bestimmten Rechtsgrundlage hin.

Der Datenschutzbeauftragte bemerkte in seiner Vernehmlassung zur Neuordnung der Pflegefinanzierung, dass keine ausreichenden Bestimmungen über die mit dem Vollzug des Gesetzes einhergehenden Datenbearbeitungen enthalten seien.

Voraussetzungen für Datenbearbeitungen

Der Gesetzgeber muss sich mit den Risiken für die Persönlichkeitsrechte einer konkreten Datenbearbeitung auseinandersetzen. Ausgangspunkt ist die Umschreibung des Zwecks der Datenbearbeitung, der sich aus der zu erfüllenden Aufgabe ergibt. Daraus ist wiederum abzuleiten, welche öffentlichen Organe welche Daten zur Verfolgung des Zwecks der Aufgabenerfüllung benötigen. Transparenz für die betroffenen Personen entsteht erst, wenn auf formellgesetzlicher Ebene folgende Punkte geregelt werden:

- Zweck der Datenbearbeitung in Relation zur Aufgabe, die das Vollzugsorgan zu erfüllen hat, sowie Zuweisung der Verantwortlichkeit an das zuständige öffentliche Organ
- Kreis der betroffenen Personen, Kategorien der bearbeiteten Daten und verwendete Mittel
- Voraussetzungen für die Bekanntgabe von Daten, Empfängerkreis und Methoden der Weitergabe
- Dauer und Form der Datenaufbewahrung sowie Sicherheitsmassnahmen
- Art und Weise, wie die Rechte betroffener Personen gewährleistet werden

Auf Grund der Anregungen des Datenschutzbeauftragten verabschiedete der Regierungsrat eine um entsprechende Bestimmungen ergänzte Vorlage zuhanden des Kantonsrats. So wurden beispielsweise je ein Katalog der Aufgaben und der Kategorien der bearbeiteten Daten verfasst. Auch wurden verschiedene Regelungen über Datenerhebungen und -weitergaben vorgesehen. Allerdings enthielt auch diese Vorlage Mängel in Bezug auf die Festlegung der Verantwortlichkeiten und zeigte einige Redundanzen mit dem IDG. Der Datenschutzbeauftragte hatte jedoch keine Möglichkeit mehr, hierzu Stellung zu nehmen.

Anforderungen nicht erfüllt

Auf Antrag der Kommission für soziale Sicherheit und Gesundheit strich der Kantonsrat diese Bestimmungen jedoch in ihrer Gesamtheit und ersetzte sie durch eine generalklauselartige Norm, wonach die Gesundheitsdirektion sämtliche Daten bearbeiten kann, die sie für den Vollzug des Gesetzes benötigt. Damit wird allerdings weder für die betroffenen Personen Transparenz geschaffen noch stellt die Bestimmung eine Vollzugshilfe für die betroffenen öffentlichen Organe dar. Der Regelung fehlt es an der nötigen Ausführlichkeit und Präzision, und die Anforderungen des IDG werden nicht erfüllt. Das IDG verlangt für das Bearbeiten und Bekanntgeben von besonderen Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz. Damit konkretisiert es das verfassungsmässige Gebot, dass ein Eingriff in die Grundrechte betroffener Personen gesetzlich geregelt und verhältnismässig sein muss.
Der Vernehmlassungsentwurf des neuen Spitalplanungs- und -finanzierungsgesetzes enthielt bereits ausführliche Datenbearbeitungsvorschriften. Der Datenschutzbeauftragte brachte in seiner Stellungnahme verschiedene Verbesserungsvorschläge ein. Das Gesetz befindet sich noch in der parlamentarischen Beratung.

§ 8 Abs. 2 IDG

§ 17 IDG

Keine Datenschutzbestimmungen im Kinder- und Jugendhilfegesetz

Eine Arbeitsgruppe hat datenschutzrechtrechtliche Bestimmungen für das neue Kinder- und Jugendhilfegesetz erarbeitet. Der Regierungsrat hat indessen entschieden, diese erst später in das Gesetz einzufügen, weshalb die aktuelle Gesetzesrevision keine hinreichenden Bestimmungen zum Schutz der betroffenen Personen enthält.

Der Entwurf zum Kinder- und Jugendhilfegesetz sieht staatliche Leistungen für Kinder, Jugendliche und Eltern vor, beispielsweise Beratung und Unterstützung im Zusammenhang mit Kinderbetreuung oder Vormundschaft. Im Rahmen dieser Aufgaben bearbeiten verschiedene Amtsstellen des Kantons und der Gemeinden sensible Personendaten über die familiären, gesundheitlichen und finanziellen Verhältnisse. Gemäss IDG setzt die Bearbeitung besonderer Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz voraus. Das IDG gewährt für die Bearbeitung bestehender Informationsbestände eine Übergangsfrist: Die Vorschrift über die formellgesetzliche Grundlage muss innert fünf Jahren umgesetzt werden, das heisst bis Oktober 2013.

Arbeitsgruppe konkretisiert Datenschutz

Das Amt für Jugend und Berufsberatung setzte deshalb eine Arbeitsgruppe ein, in der auch der Datenschutzbeauftragte mitwirkte. Die Arbeitsgruppe formulierte Datenschutzbestimmungen für das Kinder- und Jugendhilfegesetz. Darin werden die Zwecke der Datenbearbeitung aufgezählt sowie die Beschaffung, der Austausch und die Aufbewahrung der Daten geregelt. Diese Ergebnisse sind nicht in die Gesetzesvorlage des Regierungsrats eingeflossen, und so wurde diese ohne Regelung des Datenschutzes an den Kantonsrat überwiesen. Die Bestimmungen über den Datenschutz sollten später im Rahmen einer Gesetzesrevision eingefügt werden.

Verfassungsrechtliche Bedenken

Als Grund für dieses Vorgehen wurde die fünfjährige Übergangsfrist genannt. Dabei wurde nicht berücksichtigt, dass diese Übergangfrist nur für «bestehende Informationsbestände», nicht jedoch für neu geschaffene Gesetze gilt. Zudem führt eine Inkraftsetzung des – hinsichtlich des Datenschutzes – lückenhaften Kinder- und Jugendhilfegesetzes zu Rechtsunsicherheiten. Aus Gründen der Transparenz für die betroffenen Personen sollte aus dem neuen Gesetz von Anfang an ersichtlich sein, welche Datenbearbeitungen durch welche Behörden zu welchen Zwecken zulässig sind.

Der Umgang mit Daten über familiäre, gesundheitliche und finanzielle Verhältnisse greift in die Privatsphäre der betroffenen Personen ein. Gemäss der Bundesverfassung bedürfen solche Eingriffe bereits heute einer gesetzlichen Grundlage. Das IDG konkretisiert diese verfassungsrechtliche Vorgabe und verlangt für das Bearbeiten besonderer Personendaten ein formelles Gesetz. Das Fehlen solcher Bestimmungen im vorliegenden Zusammenhang führt zu unzulässigen Datenbearbeitungen und damit zu unverhätlnismässigen Eingriffen in die Privatsphäre der betroffenen Menschen.

§ 8 Abs. 2 IDG

§ 17 Abs. 1 lit. a IDG

§ 41 IDG

Gefragte Datenschutzinformationen

Im Zentrum der Informationstätigkeit des Datenschutzbeauftragten standen 2010 die Beantwortung von über hundert Medienanfragen sowie die Publikation von Beiträgen zu aktuellen Fragen des Datenschutzes.

Wie bereits in den Vorjahren lud der Datenschutzbeauftragte die Medien im Frühling 2010 zur Jahrespressekonferenz ein. Im Zentrum der Ausführungen stand dabei ein Pilotprojekt zu intelligenten Stromzählern (Smart Meters) im Kanton Zürich, bei dem im Rahmen einer Vorabkontrolle überprüft worden war, welche technischen und organisatorischen Regelungen bei dieser neuen Messtechnologie notwendig sind, um den Anforderungen des Datenschutzes Rechnung zu tragen.

Neue Technologien im Fokus der Medien

Im Berichtsjahr verzeichnete der Datenschutzbeauftragte über hundert Anfragen von Medienschaffenden aus der ganzen Schweiz. Das Thema Videoüberwachung stand dabei ganz oben auf der Hitliste der Journalistinnen und Journalisten: Die vom Datenschutzbeauftragten bearbeiteten Anfragen reichten von der Überwachung in öffentlichen Verkehrsmitteln oder rund um Schulhäuser über die Veröffentlichung von Videos aus Überwachungskameras auf Internetplattformen bis hin zur Verwendung von Videomaterial für die polizeiliche Fahndung. Weitere Schwerpunkte waren Social Networks und Internetdienste sowie der Staatsschutz.

Leitfaden zu Videoüberwachung durch öffentliche Organe publiziert

Die zahlreichen Geschäfte und Anfragen rund um die Videoüberwachung veranlassten den Datenschutzbeauftragten im Berichtsjahr, einen Leitfaden zum Thema zu publizieren. Dieser zeigt den öffentlichen Organen auf, welche Punkte sie bei einer geplanten Videoüberwachung berücksichtigen müssen. Der Leitfaden enthält zudem ein Musterreglement mit Stichwörtern zum Regelungsbedarf, das den Behörden praktische Hinweise und Unterstützung bei der Umsetzung anbietet.

Erhöhte Wirkung durch Kooperationen

Eine wichtige Kommunikationsplattform war erneut die vierteljährlich erscheinende Zeitschrift für Datenrecht und Informationssicherheit «digma», die es dem Datenschutzbeauftragten ermöglicht, eine breite Palette von datenschutzrelevanten Themen zu bearbeiten und eine vielfältige Leserschaft anzusprechen.

Sämtliche Publikationen des Datenschutzbeauftragten finden sich auch auf www.datenschutz.ch.

Erfolgreiche Kurse und Seminare

Im Berichtsjahr führte der Datenschutzbeauftragte insgesamt neun gut besuchte Weiterbildungskurse für Verwaltungsmitarbeitende des Kantons durch. Zusammen mit Partnern aus Wissenschaft und öffentlicher Hand wurden ausserdem verschiedene Veranstaltungen für unterschiedlichste Zielgruppen organisiert.

Basierend auf dem im IDG festgelegten Aufgabenkatalog bietet der Datenschutzbeauftragte eine breite Palette von Aus- und Weiterbildungsmöglichkeiten an. Die Vermittlung datenschutzrechtlicher Grundlagen, die Sensibilisierung für eines der wichtigsten Bürgerrechte einer liberalen Gesellschaft – nämlich das Recht auf einen angemessenen Schutz der Privatsphäre – sowie die Präsentation organisatorischer und technischer Instrumente stehen dabei im Zentrum. Die Angebote richten sich in erster Linie an Mitarbeitende der kantonalen Verwaltung, Bezirke und Gemeinden. Im Rahmen der jährlichen Symposiums on Privacy and Security sowie bei den regelmässig stattfindenden Referaten und Präsentationen des Datenschutzbeauftragten und seiner Mitarbeitenden soll aber auch ein breites Publikum auf die Bedeutung des Datenschutzes und des Respekts vor der Privatsphäre in einer modernen Wissens- und Informationsgesellschaft aufmerksam gemacht werden.

Informatiksicherheit und Datenschutz in der Gemeinde

2010 lancierte der Datenschutzbeauftragte das Kursmodul «Sicherheit von Informations- und Kommunikationstechnologien für Gemeinden». Insgesamt fanden im Berichtsjahr acht solche Kurse statt, an denen primär Informationssicherheitsverantwortliche von Gemeinden teilnahmen. Neben datenschutzrechtlichen Grundlagen vermittelt der Kurs einen Überblick über Sicherheitsstandards sowie organisatorische Massnahmen und präsentiert Tools zur Datensicherheit. Aufgrund der grossen Nachfrage soll die Schulung auch im kommenden Jahr angeboten werden.

Praxisorientierte Weiterbildung für Fachleute

Im Berichtsjahr organisierte der Datenschutzbeauftragte wiederum eine fachspezifische Weiterbildung für Verwaltungsangestellte im Gesundheitswesen, die mit der Bearbeitung besonders schützenswerter Personendaten betraut sind. Bei der Schulung standen die Klärung und Beantwortung rechtlicher, organisatorischer und technischer Fragestellungen der Mitarbeiterinnen und Mitarbeiter im Umgang mit Personendaten im Zentrum. Ziel ist es jeweils, den Mitarbeitenden die Grundsätze des Datenschutzes und der Datensicherheit sowie die spezifischen Problemstellungen und Geheimhaltungsbestimmungen zu vermitteln. Dabei wird auch auf aktuelle Trends und Entwicklungen im jeweiligen Fachgebiet eingegangen, und es werden Fälle aus der Praxis bearbeitet. Der Kurs wurde 2010 zum wiederholten Mal angeboten und findet einmal jährlich statt.

Zusammen mit der Koordinationsstelle IDG in der Staatskanzlei wurde im Berichtsjahr das Seminar zum Öffentlichkeitsprinzip neu lanciert. Die Weiterbildung richtet sich primär an Verwaltungsmitarbeiter ohne juristische Ausbildung und bietet praktische Hilfestellungen im Umgang mit den verschiedenen Verwaltungsinformationen. Die Vermittlung des korrekten Vorgehens bei Informationen «von Amtes wegen» sowie bei der Behandlung von Zugangsgesuchen zu Verwaltungsdokumenten stehen dabei im Zentrum der Schulung. Das Seminar zum Öffentlichkeitsprinzip soll auch in Zukunft einmal jährlich statt finden.

Zurzeit befindet sich das Aus- und Weiterbildungskonzept des Datenschutzbeauftragten in der Überarbeitung – die neuen Schwerpunkte sollen per Mitte 2011 umgesetzt werden.

Beliebte Referate und Präsentationen

Auch im Berichtsjahr nahmen der Datenschutzbeauftragte und seine Mitarbeitenden wiederum verschiedene Einladungen zu Referaten und Präsentationen zum Thema Privatheit und Datenschutz an. Wie bereits in den Vorjahren wurden dabei eine breite Palette von Fragestellungen thematisiert und ganz unterschiedliche Zielgruppen angesprochen:

Ausgewählte Referate des Datenschutzbeauftragten 2010

- Datenschutz und E-Health
- Datenschutzrechtliche Entwicklungen und Umsetzungen
- Smart Grids & Smart Meters
- Privatheit im öffentlichen Raum angesichts von Videoüberwachung und Google Street View
- Datenschutz in der digitalen Welt
- Die richtige Balance zwischen Sicherheit und Privatheit
- Vertrauenswürdiges Open Government

Data Warehouses und Data Mining im Fokus

Bereits zum 15. Mal fand Ende August 2010 in Zürich das von der Stiftung für Datenschutz und Informationssicherheit (SDI) organisierte Symposium on Privacy and Security statt. Ziel der SDI ist es, die Öffentlichkeit auf die Bedeutung von Privatheit und Sicherheit in der Informations- und Wissensgesellschaft aufmerksam zu machen sowie Bestrebungen zur Verbesserung des Datenschutzes und der Informationssicherheit zu unterstützen. Im Zentrum dieser ganztägigen Veranstaltung stand im Berichtsjahr das Thema «Data Warehouses und Data Mining». Dabei wurde aufgezeigt, wie die Zentralisierung von Informationsbearbeitungen in Privatwirtschaft und Verwaltung sowie die Möglichkeiten des interaktiven Datenaustauschs im Rahmen des Web 2.0 stetig voranschreiten und welche organisatorischen, technischen und datenschutzrechtlichen Massnahmen Privatheit und Informationssicherheit besonders wirksam schützen.

Impressum

Herausgeber
Datenschutzbeauftragter des Kantons Zürich,
Postfach, 8090 Zürich

Redaktion
Team des Datenschutzbeauftragten des Kantons Zürich

Schlussredaktion
Isabel Garcia

Korrektorat
Text Control, Zürich

Layout und Druck
Kantonale Drucksachen- und Materialzentrale Zürich

Auflage
1000

ISSN 1422-5816

Hinweis
Sämtliche personellen und/oder institutionellen Angaben zum Datenschutzbeauftragten des Kantons Zürich finden sich auf der Website www.datenschutz.ch, Rubrik «Porträt».

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